SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 September 2025

Generated on 24 September 2025

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-9588	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Iron Mountain Archiving Services Inc. EnVision allows Command Injection.This issue affects enVision: before 250563.	10.0	More Details
CVE-2025-10035	A deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection.	10.0	More Details
CVE-2025-9846	Unrestricted Upload of File with Dangerous Type vulnerability in TalentSys Consulting Information Technology Industry Inc. Inka.Net allows Command Injection.This issue affects Inka.Net: before 6.7.1.	10.0	More Details
CVE-2025-59528	Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5, Flowise is vulnerable to remote code execution. The CustomMCP node allows users to input configuration settings for connecting to an external MCP server. This node parses the user-provided mcpServerConfig string to build the MCP server configuration. However, during this process, it executes JavaScript code without any security validation. Specifically, inside the convertToValidJSONString function, user input is directly passed to the Function() constructor, which evaluates and executes the input as JavaScript code. Since this runs with full Node.js runtime privileges, it can access dangerous modules such as child_process and fs. This issue has been patched in version 3.0.6.	10.0	More Details
CVE-2024-13151	Authorization Bypass Through User-Controlled SQL Primary Key, CWE - 89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Logo Software Diva allows SQL Injection, CAPEC - 7 - Blind SQL Injection.This issue affects Diva: through 4.56.00.00.	10.0	More Details
CVE-2025-9971	Certain models of Industrial Cellular Gateway developed by Planet Technology have a Missing Authentication vulnerability, allowing unauthenticated remote attackers to manipulate the device via a specific functionality.	9.8	More Details
CVE-2025-57601	AiKaan Cloud Controller uses a single hardcoded SSH private key and the username `proxyuser` for remote terminal access to all managed IoT/edge devices. When an administrator initiates "Open Remote Terminal" from the AiKaan dashboard, the controller sends this same static private key to the target device. The device then uses it to establish a reverse SSH tunnel to a remote access server, enabling browser-based SSH access for the administrator. Because the same `proxyuser` account and SSH key are reused across all customer environments: - An attacker who obtains the key (e.g., by intercepting it in transit, extracting it from the remote access server, or from a compromised admin account) can impersonate any managed device. - They can establish unauthorized reverse SSH tunnels and interact	9.8	More Details

	with devices without the owner's consent. This is a design flaw in the authentication model: compromise of a single key compromises the trust boundary between the controller and devices.		
CVE-2025-56074	A SQL Injection vulnerability was discovered in the foreigner-bwdates-reports-details.php file of PHPGurukul Park Ticketing Management System v2.0. This vulnerability allows remote attackers to execute arbitrary SQL code via the fromdate parameter in a POST request.	9.8	More Details
CVE-2025-35042	Airship AI Acropolis includes a default administrative account that uses the same credentials on every installation. Instances of Airship AI that do not change this account password are vulnerable to a remote attacker logging in and gaining the privileges of this account. Fixed in 10.2.35, 11.0.21, and 11.1.9.	9.8	More Details
CVE-2025-57432	Blackmagic Web Presenter version 3.3 exposes a Telnet service on port 9977 that accepts unauthenticated commands. This service allows remote attackers to manipulate stream settings, including changing video modes and possibly altering device functionality. No credentials or authentication mechanisms are required to interact with the Telnet interface.	9.8	More Details
CVE-2025-57437	The Blackmagic Web Presenter HD firmware version 3.3 exposes sensitive information via an unauthenticated Telnet service on port 9977. When connected, the service reveals extensive device configuration data including: - Model, version, and unique identifiers - Network settings including IP, MAC, DNS - Current stream platform, stream key, and streaming URL - Audio/video configuration This data can be used to hijack live streams or perform network reconnaissance.	9.8	More Details
CVE-2025-57602	Insufficient hardening of the proxyuser account in the AiKaan IoT management platform, combined with the use of a shared, hardcoded SSH private key, allows remote attackers to authenticate to the cloud controller, gain interactive shell access, and pivot into other connected IoT devices. This can lead to remote code execution, information disclosure, and privilege escalation across customer environments.	9.8	More Details
CVE-2025-10412	The Product Options and Price Calculation Formulas for WooCommerce – Uni CPO (Premium) plugin for WordPress is vulnerable to arbitrary file uploads due to misconfigured file type validation in the 'uni_cpo_upload_file' function in all versions up to, and including, 4.9.54. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-57441	The Blackmagic ATEM Mini Pro 2.7 exposes sensitive device and stream configuration information via an unauthenticated Telnet service on port 9990. Upon connection, the attacker can access a protocol preamble that leaks the video mode, routing configuration, input/output labels, device model, and even internal identifiers such as the unique ID. This can be used for reconnaissance and planning further attacks.	9.8	More Details
CVE-2025-26399	SolarWinds Web Help Desk was found to be susceptible to an unauthenticated AjaxProxy deserialization remote code execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability is a patch bypass of CVE-2024-28988, which in turn is a patch bypass of CVE-2024-28986.	9.8	More Details
CVE-2025-9321	The WPCasa plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 1.4.1. This is due to insufficient input validation and restriction on the 'api_requests' function. This makes it possible for unauthenticated attackers to call arbitrary functions and execute code.	9.8	More Details
CVE-2025-9972	Certain models of Industrial Cellular Gateway developed by Planet Technology have an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the device.	9.8	More Details
CVE-2025-5948	The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's identity prior to claiming a business when using the claim_business AJAX action. This makes it possible for unauthenticated attackers to login as any user including admins. Please note that subscriber privileges or brute-forcing are needed when completing the business takeover. The claim_id is needed to takeover the admin account, but brute-forcing is a practical approach to obtaining valid IDs.	9.8	More Details
CVE-2025-23316	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause a remote code execution by manipulating the model name parameter in the model control APIs. A successful exploit of this vulnerability might lead to remote code execution, denial of service, information disclosure, and data tampering.	9.8	More Details
CVE-2025-10690	The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to unauthorized arbitrary file uploads due to a missing capability check on the 'beplus_import_pack_install_plugin' function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve remote code execution.	9.8	More Details
CVE-2025-10439	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yordam Informatics Yordam Library Automation System allows SQL Injection.This issue affects Yordam Library Automation System: from 21.5 & 21.6 before 21.7.	9.8	More Details

CVE-2025-8077	A vulnerability exists in NeuVector versions up to and including 5.4.5, where a fixed string is used as the default password for the built-in `admin` account. If this password is not changed immediately after deployment, any workload with network access within the cluster could use the default credentials to obtain an authentication token. This token can then be used to perform any operation via NeuVector APIs.	9.8	More Details
CVE-2025-59304	A directory traversal issue in Swetrix Web Analytics API 3.1.1 before 7d8b972 allows a remote attacker to achieve Remote Code Execution via a crafted HTTP request.	9.8	More Details
CVE-2025-59340	jinjava is a Java-based template engine based on django template syntax, adapted to render jinja templates. Priori to 2.8.1, by using mapper.getTypeFactory().constructFromCanonical(), it is possible to instruct the underlying ObjectMapper to deserialize attacker-controlled input into arbitrary classes. This enables the creation of semi-arbitrary class instances without directly invoking restricted methods or class literals. As a result, an attacker can escape the sandbox and instantiate classes such as java.net.URL, opening up the ability to access local files and URLs(e.g., file:///etc/passwd). With further chaining, this primitive can potentially lead to remote code execution (RCE). This vulnerability is fixed in 2.8.1.	9.8	More Details
CVE-2025-59352	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the gRPC API and HTTP APIs allow peers to send requests that force the recipient peer to create files in arbitrary file system locations, and to read arbitrary files. This allows peers to steal other peers' secret data and to gain remote code execution (RCE) capabilities on the peer's machine.This vulnerability is fixed in 2.1.0.	9.8	More Details
CVE-2025-10147	The Podlove Podcast Publisher plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'move_as_original_file' function in all versions up to, and including, 4.2.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-5305	The Password Reset with Code for WordPress REST API WordPress plugin before 0.0.17 does not use cryptographically sound algorithms to generate OTP codes, potentially leading to account takeovers.	9.8	More Details
CVE-2025-9083	The Ninja Forms WordPress plugin before 3.11.1 unserializes user input via form field, which could allow Unauthenticated users to perform PHP Object Injection when a suitable gadget is present on the blog.	9.8	More Details
CVE-2025-30519	Dover Fueling Solutions ProGauge MagLink LX4 Devices have default root credentials that cannot be changed through standard administrative means. An attacker with network access to the device can gain administrative access to the system.	9.8	More Details
CVE-2025-54807	The secret used for validating authentication tokens is hardcoded in device firmware for affected versions. An attacker who obtains the signing key can bypass authentication, gaining complete access to the system.	9.8	More Details
CVE-2025-58255	Cross-Site Request Forgery (CSRF) vulnerability in yonisink Custom Post Type Images allows Code Injection. This issue affects Custom Post Type Images: from n/a through 0.5.	9.6	More Details
CVE-2025-59434	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to August 2025 Cloud-Hosted Flowise, an authenticated vulnerability in Flowise Cloud allows any user on the free tier to access sensitive environment variables from other tenants via the Custom JavaScript Function node. This includes secrets such as OpenAI API keys, AWS credentials, Supabase tokens, and Google Cloud secrets — resulting in a full cross-tenant data exposure. This issue has been patched in the August 2025 Cloud-Hosted Flowise.	9.6	More Details
CVE-2025-8942	The WP Hotel Booking WordPress plugin before 2.2.3 lacks proper server-side validation for review ratings, allowing an attacker to manipulate the rating value (e.g., sending negative or out-of-range values) by intercepting and modifying requests.	9.1	More Details
CVE-2025-40925	Starch versions 0.14 and earlier generate session ids insecurely. The default session id generator returns a SHA-1 hash seeded with a counter, the epoch time, the built-in rand function, the PID, and internal Perl reference addresses. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems.	9.1	More Details
CVE-2025-57644	Accela Automation Platform 22.2.3.0.230103 contains multiple vulnerabilities in the Test Script feature. An authenticated administrative user can execute arbitrary Java code on the server, resulting in remote code execution. In addition, improper input validation allows for arbitrary file write and server-side request forgery (SSRF), enabling interaction with internal or external systems. Successful exploitation can lead to full server compromise, unauthorized access to sensitive data, and further network exploitation.	9.1	More Details
CVE-2025-48703	CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1205 allows unauthenticated remote code execution via shell metacharacters in the t_total parameter in a filemanager changePerm request.	9.0	More Details

	A valid non-root username must be known.		
CVE-2025-58766	Dyad is a local AI app builder. A critical security vulnerability has been discovered that affected Dyad v0.19.0 and earlier versions that allows attackers to execute arbitrary code on users' systems. The vulnerability affects the application's preview window functionality and can bypass Docker container protections. An attacker can craft web content that automatically executes when the preview loads. The malicious content can break out of the application's security boundaries and gain control of the system. This has been fixed in Dyad v0.20.0 and later.	9.0	More Details
CVE-2025-59545	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, the Prompt module allows execution of commands that can return raw HTML. Malicious input, even if sanitized for display elsewhere, can be executed when processed through certain commands, leading to potential script execution (XSS). This issue has been patched in version 10.1.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-9798	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Netcad Software Inc. Netigma allows Stored XSS.This issue affects Netigma: from 6.3.3 before 6.3.5 V8.	8.9	More Details
CVE-2025-57605	Lack of server-side authorisation on department admin assignment APIs in AiKaan IoT Platform allows authenticated users to elevate their privileges by assigning themselves as admins of other departments. This results in unauthorized privilege escalation across the department	8.8	More Details
CVE-2025-9216	The StoreEngine – Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the import() function in all versions up to, and including, 1.5.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-10792	A security vulnerability has been detected in D-Link DIR-513 A1FW110. Affected is an unknown function of the file /goform/formWPS. Such manipulation of the argument webpage leads to buffer overflow. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-10205	Use of a One-Way Hash with a Predictable Salt vulnerability in ABB FLXEON.This issue affects FLXEON: through 9.3.5. and newer versions	8.8	More Details
CVE-2025-59572	Cross-Site Request Forgery (CSRF) vulnerability in purethemes WorkScout-Core allows Cross Site Request Forgery. This issue affects WorkScout-Core: from n/a through n/a.	8.8	More Details
CVE-2025-57293	A command injection vulnerability in COMFAST CF-XR11 (firmware V2.7.2) exists in the multi_pppoe API, processed by the sub_423930 function in /usr/bin/webmgnt. The phy_interface parameter is not sanitized, allowing attackers to inject arbitrary commands via a POST request to /cgi-bin/mbox-config?method=SET&section=multi_pppoe. When the action parameter is set to "one_click_redial", the unsanitized phy_interface is used in a system() call, enabling execution of malicious commands. This can lead to unauthorized access to sensitive files, execution of arbitrary code, or full device compromise.	8.8	More Details
CVE-2025-10756	A security flaw has been discovered in UTT HiPER 840G up to 3.1.1-190328. Impacted is an unknown function of the file /goform/getOneApConfTempEntry. The manipulation of the argument tempName results in buffer overflow. It is possible to launch the attack 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.	8.8	More Details
CVE-2025-10757	A weakness has been identified in UTT 1200GW up to 3.0.0-170831. The affected element is an unknown function of the file /goform/formConfigDnsFilterGlobal. This manipulation of the argument GroupName causes buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-10666	A security flaw has been discovered in D-Link DIR-825 up to 2.10. Affected by this vulnerability is the function sub_4106d4 of the file apply.cgi. The manipulation of the argument countdown_time results in buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-53969	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a service implementing a proprietary protocol on TCP port 1069 to allow the client-side software, such as the In-Sight Explorer tool, to perform management operations such as changing network settings or modifying users' access to the device.	8.8	More Details

CVE-2025-10815	A vulnerability was identified in Tenda AC20 up to 16.03.08.12. Affected by this issue is the function strcpy of the file /goform/SetPptpServerCfg of the component HTTP POST Request Handler. Such manipulation of the argument startIp leads to buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-10380	The Advanced Views – Display Posts, Custom Fields, and More plugin for WordPress is vulnerable to Server-Side Template Injection in all versions up to, and including, 3.7.19. This is due to insufficient input sanitization and lack of access control when processing custom Twig templates in the Model panel. This makes it possible for authenticated attackers, with author-level access or higher, to execute arbitrary PHP code and commands on the server.	8.8	More Details
CVE-2025-9844	Uncontrolled Search Path Element vulnerability in Salesforce Salesforce CLI on Windows allows Replace Trusted Executable.This issue affects Salesforce CLI: before 2.106.6.	8.8	More Details
CVE-2025-10779	A vulnerability was found in D-Link DCS-935L up to 1.13.01. The impacted element is the function sub_402280 of the file /HNAP1/. The manipulation of the argument HNAP_AUTH/SOAPAction results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-10773	A security flaw has been discovered in B-Link BL-AC2100 up to 1.0.3. Affected by this issue is the function delshrpath of the file /goform/set_delshrpath_cfg of the component Web Management Interface. The manipulation of the argument Type results in stack-based buffer overflow. The attack may be performed from remote. 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.	8.8	More Details
CVE-2025-10838	A vulnerability was identified in Tenda AC21 16.03.08.16. The affected element is the function sub_45BB10 of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-9900	A flaw was found in Libtiff. This vulnerability is a "write-what-where" condition, triggered when the library processes a specially crafted TIFF image file. By providing an abnormally large image height value in the file's metadata, an attacker can trick the library into writing attacker-controlled color data to an arbitrary memory location. This memory corruption can be exploited to cause a denial of service (application crash) or to achieve arbitrary code execution with the permissions of the user.	8.8	More Details
CVE-2025-10803	A vulnerability has been found in Tenda AC23 up to 16.03.07.52. Affected by this vulnerability is the function sscanf of the file /goform/SetPptpServerCfg of the component HTTP POST Request Handler. Such manipulation of the argument startIp leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-10057	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.28. This is due to the write_to_customfile() function writing unfiltered PHP code to a file. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject the customFunction.php file with PHP code that can be accessed to trigger remote code execution.	8.8	More Details
CVE-2025-10589	The N-Reporter, N-Cloud, and N-Probe developed by N-Partner has an OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	8.8	More Details
CVE-2023-49564	The CBIS/NCS Manager API is vulnerable to an authentication bypass. By sending a specially crafted HTTP header, an unauthenticated user can gain unauthorized access to API functions. This flaw allows attackers to reach restricted or sensitive endpoints of the HTTP API without providing any valid credentials. The root cause of this vulnerability lies in a weak verification mechanism within the authentication implementation present in the Nginx Podman container on the CBIS/NCS Manager host machine. The risk can be partially mitigated by restricting access to the management network using external firewall.	8.8	More Details
CVE-2025-52159	Hardcoded credentials in default configuration of PPress 0.0.9.	8.8	More Details
CVE-2025-58244	Cross-Site Request Forgery (CSRF) vulnerability in Anps Constructo allows Object Injection. This issue affects Constructo: from n/a through 4.3.9.	8.8	More Details
CVE-2025-58250	Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Authentication Bypass. This issue affects Findgo: from n/a through 1.3.55.	8.8	More Details
CVE-2025-	Server-side template injection (SSTI) vulnerability in PPress 0.0.9 allows attackers to execute arbitrary code	8.8	More

54815	via crafted themes.		Details
CVE-2025-57431	The Sound4 PULSE-ECO AES67 1.22 web-based management interface is vulnerable to Remote Code Execution (RCE) via a malicious firmware update package. The update mechanism fails to validate the integrity of manual.sh, allowing an attacker to inject arbitrary commands by modifying this script and repackaging the firmware.	8.8	More Details
CVE-2025-58013	Cross-Site Request Forgery (CSRF) vulnerability in pebas CouponXxL allows Privilege Escalation. This issue affects CouponXxL: from n/a through 4.5.0.	8.8	More Details
CVE-2025-10647	The Embed PDF for WPForms plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajax_handler_download_pdf_media function in all versions up to, and including, 1.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-57439	Creacast Creabox Manager 4.4.4 contains a critical Remote Code Execution vulnerability accessible via the edit.php endpoint. An authenticated attacker can inject arbitrary Lua code into the configuration, which is then executed on the server. This allows full system compromise, including reverse shell execution or arbitrary command execution.	8.8	More Details
CVE-2025-43953	In 2wcom IP-4c 2.16, the web interface allows admin and manager users to execute arbitrary code as root via a ping or traceroute field on the TCP/IP screen.	8.8	More Details
CVE-2023-49367	An issue in user interface in Kyocera Command Center RX EXOSYS M5521cdn allows remote to obtain sensitive information via inspecting sent packages by user.	8.8	More Details
CVE-2025-57434	Creacast Creabox Manager contains a critical authentication flaw that allows an attacker to bypass login validation. The system grants access when the username is creabox and the password begins with the string creacast, regardless of what follows.	8.8	More Details
CVE-2025-10244	A maliciously crafted HTML payload, when rendered by the Autodesk Fusion desktop application, can trigger a Stored Cross-site Scripting (XSS) vulnerability. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	8.7	More Details
CVE-2025-53468	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in gopiplus@hotmail.com Wp tabber widget allows SQL Injection. This issue affects Wp tabber widget: from n/a through 4.0.	8.5	More Details
CVE-2025-58686	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in quadlayers Perfect Brands for WooCommerce allows SQL Injection. This issue affects Perfect Brands for WooCommerce: from n/a through 3.6.0.	8.5	More Details
CVE-2023-49565	The cbis_manager Podman container is vulnerable to remote command execution via the /api/plugins endpoint. Improper sanitization of the HTTP Headers X-FILENAME, X-PAGE, and X-FIELD allows for command injection. These headers are directly utilized within the subprocess.Popen Python function without adequate validation, enabling a remote attacker to execute arbitrary commands on the underlying system by crafting malicious header values within an HTTP request to the affected endpoint. The web service executes with root privileges within the container environment, the demonstrated remote code execution permits an attacker to acquire elevated privileges for the command execution. Restricting access to the management network with an external firewall can partially mitigate this risk.	8.4	More Details
CVE-2025-59458	In JetBrains Junie before 252.284.66, 251.284.66, 243.284.66, 252.284.61, 251.284.61, 243.284.61, 252.284.50, 252.284.54, 251.284.54, 251.284.50, 243.284.54, 243.284.50 code execution was possible due to improper command validation	8.3	More Details
CVE-2025-55069	A predictable seed in pseudo-random number generator vulnerability has been discovered in firmware version 3.60 of the Click Plus PLC. The vulnerability relies on the fact that the software implements a predictable seed for its pseudo-random number generator, which compromises the security of the generated private keys.	8.3	More Details
CVE-2025-59484	The use of a broken or risky cryptographic algorithm was discovered in firmware version 3.60 of the Click Plus PLC. The vulnerability relies on the fact that the software uses an insecure implementation of the RSA encryption algorithm.	8.3	More Details
CVE-2025-55068	Dover Fueling Solutions ProGauge MagLink LX4 Devices fail to handle Unix time values beyond a certain point. An attacker can manually change the system time to exploit this limitation, potentially causing errors in authentication and leading to a denial-of-service condition.	8.2	More Details
	Mesh Connect JS SDK contains JS libraries for integrating with Mesh Connect. Prior to version 3.3.2, the lack of		

CVE-2025-59430	sanitization of URLs protocols in the createLink.openLink function enables the execution of arbitrary JavaScript code within the context of the parent page. This is technically indistinguishable from a real page at the rendering level and allows access to the parent page DOM, storage, session, and cookies. If the attacker can specify customIframeId, they can hijack the source of existing iframes. This issue has been patched in version 3.3.2.	8.2	More Details
CVE-2025-5955	The Service Finder SMS System plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.0. This is due to the plugin not verifying a user's phone number before logging them in. This makes it possible for unauthenticated attackers to login as arbitrary users.	8.1	More Details
CVE-2025-7665	The Miniorange OTP Verification with Firebase plugin for WordPress is vulnerable to privilege escalation due to a missing capability check on the 'handle_mofirebase_form_options' function in versions 3.1.0 to 3.6.2. This makes it possible for unauthenticated attackers to update the default role to Administrator. Premium features must be enabled in order to exploit the vulnerability.	8.1	More Details
CVE-2025-10058	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the upload_function() function in all versions up to, and including, 7.27. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.1	More Details
CVE-2025-54497	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a telnet-based service on port 23 to allow management operations such as firmware upgrades and device reboots, which require authentication. A user with protected privileges can successfully invoke the SetSerialPort functionality to modify relevant device properties (such as serial interface settings), contradicting the security model proposed in the user manual.	8.1	More Details
CVE-2025-52873	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a telnet-based service on port 23 to allow management operations such as firmware upgrades and device reboots, which require authentication. A user with protected privileges can successfully invoke the SetSystemConfig functionality to modify relevant device properties (such as network settings), contradicting the security model proposed in the user manual.	8.1	More Details
CVE-2025-10854	The txtai framework allows the loading of compressed tar files as embedding indices. While the validate function is intended to prevent path traversal vulnerabilities by ensuring safe filenames, it does not account for symbolic links within the tar file. An attacker is able to write a file anywhere in the filesystem when txtai is used to load untrusted embedding indices	8.1	More Details
CVE-2025-8565	The Privacy Policy Generator, Terms & Conditions Generator WordPress Plugin : WP Legal Pages plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on the wplp_gdpr_install_plugin_ajax_handler() function in all versions up to, and including, 3.4.3. This makes it possible for authenticated attackers, with Contributor-level access and above, to install arbitrary repository plugins.	8.1	More Details
CVE-2025-9079	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.10.x <= 10.10.1, 10.9.x <= 10.9.3 fail to validate import directory path configuration which allows admin users to execute arbitrary code via malicious plugin upload to prepackaged plugins directory	8.0	More Details
CVE-2025-54754	An attacker with adjacent access, without authentication, can exploit this vulnerability to retrieve a hard-coded password embedded in publicly available software. This password can then be used to decrypt sensitive network traffic, affecting the Cognex device.	8.0	More Details
CVE-2025-54761	An issue was discovered in PPress 0.0.9 allowing attackers to gain escilated privlidges via crafted session cookie.	8.0	More Details
CVE-2025-54818	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a proprietary protocol on TCP port 1069 to perform management operations such as modifying system properties. The user management functionality handles sensitive data such as registered usernames and passwords over an unencrypted channel, allowing an adjacent attacker to intercept valid credentials to gain access to the device.	8.0	More Details
CVE-2025-57295	H3C devices running firmware version NX15V100R015 are vulnerable to unauthorized access due to insecure default credentials. The root user account has no password set, and the H3C user account uses the default password "admin," both stored in the /etc/shadow file. Attackers with network access can exploit these credentials to gain unauthorized root-level access to the device via the administrative interface or other network services, potentially leading to privilege escalation, information disclosure, or arbitrary code execution.	8.0	More Details
CVE-2025-59518	In LemonLDAP::NG before 2.16.7 and 2.17 through 2.21 before 2.21.3, OS command injection can occur in the Safe jail. It does not Localize _ during rule evaluation. Thus, an administrator who can edit a rule evaluated by the Safe jail can execute commands on the server.	8.0	More Details
CVE-2025-23268	NVIDIA Triton Inference Server contains a vulnerability in the DALI backend where an attacker may cause an improper input validation issue. A successful exploit of this vulnerability may lead to code execution.	8.0	More Details

CVE-2025-54810	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a proprietary protocol on TCP port 1069 to perform management operations such as modifying system properties. The user management functionality handles sensitive data such as registered usernames and passwords over an unencrypted channel, allowing an adjacent attacker to intercept valid credentials to gain access to the device.	8.0	More Details
CVE-2025-8354	A maliciously crafted RFA file, when parsed through Autodesk Revit, can force a Type Confusion vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-9450	A Use of Uninitialized Variable vulnerability affecting the JT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025 could allow an attacker to execute arbitrary code while opening a specially crafted JT file.	7.8	More Details
CVE-2025-10672	A vulnerability was found in whuan132 AIBattery up to 1.0.9. The affected element is an unknown function of the file AIBatteryHelper/XPC/BatteryXPCService.swift of the component com.collweb.AIBatteryHelper. The manipulation results in missing authentication. The attack requires a local approach. The exploit has been made public and could be used.	7.8	More Details
CVE-2025-8892	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-51006	Within tcpreplay's tcprewrite, a double free vulnerability has been identified in the dlt_linuxsll2_cleanup() function in plugins/dlt_linuxsll2/linuxsll2.c. This vulnerability is triggered when tcpedit_dlt_cleanup() indirectly invokes the cleanup routine multiple times on the same memory region. By supplying a specifically crafted pcap file to the tcprewrite binary, a local attacker can exploit this flaw to cause a Denial of Service (DoS) via memory corruption.	7.8	More Details
CVE-2025-50255	Cross Site Request Forgery (CSRF) vulnerability in Smartvista BackOffice SmartVista Suite 2.2.22 via crafted GET request.	7.8	More Details
CVE-2025-9447	An Out-Of-Bounds Read vulnerability affecting the PAR file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025 could allow an attacker to execute arbitrary code while opening a specially crafted PAR file.	7.8	More Details
CVE-2025-58432	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.4.1 and all prior versions, the /v2_1/files/file/uploadV2 endpoint allows file upload from ANY USER who has access to localhost. File uploads are performed AS ROOT.	7.8	More Details
CVE-2025-9449	A Use After Free vulnerability affecting the PAR file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025 could allow an attacker to execute arbitrary code while opening a specially crafted PAR file.	7.8	More Details
CVE-2025-59457	In JetBrains TeamCity before 2025.07.2 missing Git URL validation allowed credential leakage on Windows	7.7	More Details
CVE-2025-59344	AliasVault is a privacy-first password manager with built-in email aliasing. A server-side request forgery (SSRF) vulnerability exists in the favicon extraction feature of AliasVault API versions 0.23.0 and lower. The extractor fetches a user-supplied URL, parses the returned HTML, and follows <link rel="icon" href="...">. Although the initial URL is validated to allow only HTTP/HTTPS with default ports, the extractor automatically follows redirects and does not block requests to loopback or internal IP ranges. An authenticated, low-privileged user can exploit this behavior to coerce the backend into making HTTP(S) requests to arbitrary internal hosts and non-default ports. If the target host serves a favicon or any other valid image, the response is returned to the attacker in Base64 form. Even when no data is returned, timing and error behavior can be abused to map internal services. This vulnerability only affects self-hosted AliasVault instances that are reachable from the public internet with public user registration enabled. Private/internal deployments without public sign-ups are not directly exploitable. This issue has been fixed in AliasVault release 0.23.1.	7.7	More Details
CVE-2025-54860	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a telnet-based service on port 23 in order to allow management operations on the device such as firmware upgrades and device reboot requiring an authentication. A wrong management of login failures of the service allows a denial-of-service attack, leaving the telnet service into an unreachable state.	7.7	More Details
CVE-2025-5962	A flaw was found in the Lightspeed history service. Insufficient access controls allow a local, unprivileged user to access and manipulate the chat history of another user on the same system. By abusing inter-process communication calls to the history service, an attacker can view, delete, or inject arbitrary history entries, including misleading or malicious commands. This can be used to deceive another user into executing harmful actions, posing a risk of privilege misuse or unauthorized command execution through social engineering.	7.7	More Details

CVE-2025-53947	A local attacker with low privileges on the Windows system where the software is installed can exploit this vulnerability to corrupt sensitive data. A data folder is created with very weak privileges, allowing any user logged into the Windows system to modify its content.	7.7	More Details
CVE-2025-57528	An issue was discovered in Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01 allowing attackers to cause a denial of service via the funcname, funcpara1, funcpara2 parameters to the formSetCfm function (uri path: SetCfm).	7.7	More Details
CVE-2025-59826	Flag Forge is a Capture The Flag (CTF) platform. In version 2.1.0, non-admin users can create arbitrary challenges, potentially introducing malicious, incorrect, or misleading content. This issue has been patched in version 2.2.0.	7.6	More Details
CVE-2025-59570	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFunnels Mail Mint allows SQL Injection. This issue affects Mail Mint: from n/a through 1.18.6.	7.6	More Details
CVE-2025-10458	Parameters are not validated or sanitized, and are later used in various internal operations.	7.6	More Details
CVE-2025-7403	Unsafe handling in bt_conn_tx_processor causes a use-after-free, resulting in a write-before-zero. The written 4 bytes are attacker-controlled, enabling precise memory corruption.	7.6	More Details
CVE-2025-59588	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PenciDesign Soledad allows PHP Local File Inclusion. This issue affects Soledad: from n/a through 8.6.8.	7.5	More Details
CVE-2025-40933	Apache::AuthAny::Cookie v0.201 or earlier for Perl generates session ids insecurely. Session ids are generated using an MD5 hash of the epoch time and a call to the built-in rand function. The epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems.	7.5	More Details
CVE-2025-58767	REXML is an XML toolkit for Ruby. The REXML gems from 3.3.3 to 3.4.1 has a DoS vulnerability when parsing XML containing multiple XML declarations. If you need to parse untrusted XMLs, you may be impacted to these vulnerabilities. The REXML gem 3.4.2 or later include the patches to fix these vulnerabilities.	7.5	More Details
CVE-2025-58973	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in hashthemes Easy Elementor Addons allows PHP Local File Inclusion. This issue affects Easy Elementor Addons: from n/a through 2.2.8.	7.5	More Details
CVE-2025-35041	Airship AI Acropolis allows unlimited MFA attempts for 15 minutes after a user has logged in with valid credentials. A remote attacker with valid credentials could brute-force the 6-digit MFA code. Fixed in 10.2.35, 11.0.21, and 11.1.9.	7.5	More Details
CVE-2025-36202	IBM webMethods Integration 10.15 and 11.1 could allow an authenticated user with required execute Services to execute commands on the system due to the improper validation of format string strings passed as an argument from an external source.	7.5	More Details
CVE-2025-23329	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause memory corruption by identifying and accessing the shared memory region used by the Python backend. A successful exploit of this vulnerability might lead to denial of service.	7.5	More Details
CVE-2025-10468	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Beyaz Computer CityPlus allows Path Traversal.This issue affects CityPlus: before 24.29375.	7.5	More Details
CVE-2025-59420	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.4, Authlib's JWS verification accepts tokens that declare unknown critical header parameters (crit), violating RFC 7515 "must-understand" semantics. An attacker can craft a signed token with a critical header (for example, bork or cnf) that strict verifiers reject but Authlib accepts. In mixed-language fleets, this enables split-brain verification and can lead to policy bypass, replay, or privilege escalation. This issue has been patched in version 1.6.4.	7.5	More Details
CVE-2025-23328	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause an out-of-bounds write through a specially crafted input. A successful exploit of this vulnerability might lead to denial of service.	7.5	More Details
CVE-2025-26515	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 without Single Sign-on enabled are susceptible to a Server-Side Request Forgery (SSRF) vulnerability. Successful exploit could allow an unauthenticated attacker to change the password of any Grid Manager or Tenant Manager non-federated user.	7.5	More Details

CVE-2025-57430	Creacast Creabox Manager 4.4.4 exposes sensitive configuration data via a publicly accessible endpoint /get. When accessed, this endpoint returns internal configuration including the creacodec.lua file, which contains plaintext admin credentials.	7.5	More Details
CVE-2025-57925	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in immonex immonex Kickstart Team allows PHP Local File Inclusion. This issue affects immonex Kickstart Team: from n/a through 1.6.9.	7.5	More Details
CVE-2025-53450	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Pluginwale Easy Pricing Table WP allows PHP Local File Inclusion. This issue affects Easy Pricing Table WP: from n/a through 1.1.3.	7.5	More Details
CVE-2025-10143	The Catch Dark Mode plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.0 via the 'catch_dark_mode' 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-2025-59527	Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5, a Server-Side Request Forgery (SSRF) vulnerability was discovered in the /api/v1/fetch-links endpoint of the Flowise application. This vulnerability allows an attacker to use the Flowise server as a proxy to access internal network web services and explore their link structures. This issue has been patched in version 3.0.6.	7.5	More Details
CVE-2025-59353	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, a peer can obtain a valid TLS certificate for arbitrary IP addresses, effectively rendering the mTLS authentication useless. The issue is that the Manager’s Certificate gRPC service does not validate if the requested IP addresses “belong to” the peer requesting the certificate—that is, if the peer connects from the same IP address as the one provided in the certificate request. This vulnerability is fixed in 2.1.0.	7.5	More Details
CVE-2025-59348	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the processPieceFromSource method does not update the structure’s usedTraffic field, because an uninitialized variable n is used as a guard to the AddTraffic method call, instead of the result.Size variable. A task is processed by a peer. The usedTraffic metadata is not updated during the processing. Rate limiting is incorrectly applied, leading to a denial-of-service condition for the peer. This vulnerability is fixed in 2.1.0.	7.5	More Details
CVE-2025-55888	Cross-Site Scripting (XSS) vulnerability was discovered in the Ajax transaction manager endpoint of ARD. An attacker can intercept the Ajax response and inject malicious JavaScript into the accountName field. This input is not properly sanitized or encoded when rendered, allowing script execution in the context of users browsers. This flaw could lead to session hijacking, cookie theft, and other malicious actions.	7.3	More Details
CVE-2025-10663	A vulnerability was found in PHPGurukul Online Course Registration 3.1. This affects an unknown function of the file /my-profile.php. Performing manipulation of the argument cgpa results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10795	A vulnerability has been found in code-projects Online Bidding System 1.0. This affects an unknown part of the file /administrator/bidupdate.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10603	A vulnerability was determined in PHPGurukul Online Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_forum/search_result.php. Executing manipulation of the argument Search can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10796	A vulnerability was found in code-projects Hostel Management System 1.0. This vulnerability affects unknown code of the file /justines/admin/login.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10621	A vulnerability was determined in SourceCodester Hotel Reservation System 1.0. The affected element is an unknown function of the file editroomimage.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10797	A vulnerability was determined in code-projects Hostel Management System 1.0. This issue affects some unknown processing of the file /justines/index.php. This manipulation of the argument log_email causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10624	A security flaw has been discovered in PHPGurukul User Management System 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument emailid results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10798	A vulnerability was identified in code-projects Hostel Management System 1.0. Impacted is an unknown function of the file /justines/admin/mod_roomtype/index.php?view=view. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details

CVE-2025-10712	A vulnerability was found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 20250831. This issue affects some unknown processing of the file /index.php/Login/login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-10604	A vulnerability was identified in PHPGurukul Online Discussion Forum 1.0. This affects an unknown part of the file /admin/edit_member.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10799	A security flaw has been discovered in code-projects Hostel Management System 1.0. The affected element is an unknown function of the file /justines/admin/mod_reservation/index.php?view=view. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10664	A vulnerability was determined in PHPGurukul Small CRM 4.0. This impacts an unknown function of the file /create-ticket.php. Executing manipulation of the argument subject can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10810	A vulnerability was detected in Campcodes Online Learning Management System 1.0. The impacted element is an unknown function of the file /admin/edit_user.php. Performing manipulation of the argument firstname results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-10667	A weakness has been identified in itsourcecode Online Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /members/compose_msg.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10800	A weakness has been identified in itsourcecode Online Discussion Forum 1.0. The impacted element is an unknown function of the file /index.php. Executing manipulation of the argument email/password can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10801	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown function of the file /admin/edit_tax.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10808	A weakness has been identified in Campcodes Farm Management System 1.0. Impacted is an unknown function of the file /uploadProduct.php. This manipulation of the argument Type causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10668	A security vulnerability has been detected in itsourcecode Online Discussion Forum 1.0. This affects an unknown part of the file /members/compose_msg_admin.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10802	A flaw has been found in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /administrator/remove.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10670	A flaw has been found in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This issue affects some unknown processing of the file /check_profile.php. Executing manipulation of the argument profile_id can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-59534	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.2, there is a command Injection vulnerability in initialize_kerberos_keytab_file_login(). The vulnerability exists because the code directly interpolates user-controlled input into a shell command and executes it via system() without any sanitization or validation. This issue has been patched in version 1.4.2.	7.3	More Details
CVE-2025-10673	A vulnerability was determined in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/class/index.php. This manipulation of the argument classId causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-	A security vulnerability has been detected in Campcodes Online Learning Management System 1.0. The		

2025-10809	affected element is an unknown function of the file /admin/department.php. Such manipulation of the argument d leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10811	A flaw has been found in code-projects Hostel Management System 1.0. This affects an unknown function of the file /justines/admin/mod_comments/index.php?view=view. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10600	A flaw has been found in SourceCodester Online Exam Form Submission 1.0. This impacts an unknown function of the file /register.php. This manipulation of the argument img causes unrestricted upload. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10857	A security flaw has been discovered in Campcodes Point of Sale System POS 1.0. Affected by this issue is some unknown functionality of the file /login.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10599	A security flaw has been discovered in itsourcecode Web-Based Internet Laboratory Management System 1.0. Impacted is the function User::AuthenticateUser of the file login.php. Performing manipulation of the argument user_email results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10784	A security vulnerability has been detected in Campcodes Online Learning Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_subject.php. The manipulation of the argument subject_code leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10813	A vulnerability was found in code-projects Hostel Management System 1.0. Affected is an unknown function of the file /justines/admin/mod_reports/index.php. The manipulation of the argument Home results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10816	A security flaw has been discovered in Jinher OA 2.0. This affects an unknown part of the file /c6/Jhsoft.Web.module/ToolBar/GetWordFileName.aspx/?text=GetUrl&style=add of the component XML Handler. Performing manipulation results in xml external entity reference. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10817	A weakness has been identified in Campcodes Online Learning Management System 1.0. This vulnerability affects unknown code of the file /admin/admin_user.php. Executing manipulation of the argument firstname can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10598	A vulnerability was identified in SourceCodester Pet Grooming Management Software 1.0. This issue affects some unknown processing of the file /admin/search_product.php. Such manipulation of the argument group_id leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10782	A security flaw has been discovered in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/class.php. Performing manipulation of the argument class_name results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10829	A vulnerability was detected in Campcodes Computer Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/sup_edit1.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	7.3	More Details
CVE-2025-10830	A flaw has been found in Campcodes Computer Sales and Inventory System 1.0. This issue affects some unknown processing of the file /pages/inv_edit1.php. Executing manipulation of the argument idd can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10831	A vulnerability has been found in Campcodes Computer Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/pro_edit1.php. The manipulation of the argument prodcode leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10832	A vulnerability was found in SourceCodester Pet Grooming Management Software 1.0. The affected element is an unknown function of the file /admin/fetch_product_details.php. The manipulation of the argument barcode results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10781	A vulnerability was identified in Campcodes Online Learning Management System 1.0. This impacts an unknown function of the file /admin/edit_class.php. Such manipulation of the argument class_name leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details

CVE-2025-10833	A vulnerability was determined in 1000projects Bookstore Management System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument unm causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10834	A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. This affects an unknown function of the file /jobportal/admin/login.php. Such manipulation of the argument user_email leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10836	A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. Affected is an unknown function of the file /admin/print1.php. Executing manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10841	A security vulnerability has been detected in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/weweee.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-10842	A vulnerability was detected in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /administrator/wew.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-10843	A flaw has been found in Reservation Online Hotel Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /reservation/paypalpayout.php. Executing manipulation of the argument confirm can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-9905	The Keras Model.load_model method can be exploited to achieve arbitrary code execution, even with safe_mode=True. One can create a specially crafted .h5/.hdf5 model archive that, when loaded via Model.load_model, will trigger arbitrary code to be executed. This is achieved by crafting a special .h5 archive file that uses the Lambda layer feature of keras which allows arbitrary Python code in the form of pickled code. The vulnerability comes from the fact that the safe_mode=True option is not honored when reading .h5 archives. Note that the .h5/.hdf5 format is a legacy format supported by Keras 3 for backwards compatibility.	7.3	More Details
CVE-2025-9906	The Keras Model.load_model method can be exploited to achieve arbitrary code execution, even with safe_mode=True. One can create a specially crafted .keras model archive that, when loaded via Model.load_model, will trigger arbitrary code to be executed. This is achieved by crafting a special config.json (a file within the .keras archive) that will invoke keras.config.enable_unsafe_deserialization() to disable safe mode. Once safe mode is disable, one can use the Lambda layer feature of keras, which allows arbitrary Python code in the form of pickled code. Both can appear in the same archive. Simply the keras.config.enable_unsafe_deserialization() needs to appear first in the archive and the Lambda with arbitrary code needs to be second.	7.3	More Details
CVE-2025-10851	A security flaw has been discovered in Campcodes Gym Management System 1.0. Impacted is an unknown function of the file /ajax.php?action=login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-10812	A vulnerability has been found in code-projects Hostel Management System 1.0. This impacts an unknown function of the file /justines/admin/mod_amenities/index.php?view=view. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10783	A weakness has been identified in Campcodes Online Learning Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add_subject.php. Executing manipulation of the argument subject_code can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10601	A vulnerability has been found in SourceCodester Online Exam Form Submission 1.0. Affected is an unknown function of the file /admin/index.php. Such manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-10785	A vulnerability was detected in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown part of the file /manage_user.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-10597	A vulnerability was determined in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. This vulnerability affects unknown code of the file /Profilers/PriProfile/COUNT2.php. This manipulation of the argument cname causes sql injection. The attack may be initiated remotely. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available.	7.3	More Details
	A vulnerability was detected in code-projects E-Commerce Website 1.0. Affected by this vulnerability is an		

CVE-2025-10793	unknown functionality of the file /pages/admin_account_delete.php. Performing manipulation of the argument user_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-59424	LinkAce is a self-hosted archive to collect website links. Prior to 2.3.1, a Stored Cross-Site Scripting (XSS) vulnerability has been identified on the /system/audit page. The application fails to properly sanitize the username field before it is rendered in the audit log. An authenticated attacker can set a malicious JavaScript payload as their username. When an action performed by this user is recorded (e.g., generate or revoke an API token), the payload is stored in the database. The script is then executed in the browser of any user, particularly administrators, who views the /system/audit page. This vulnerability is fixed in 2.3.1.	7.3	More Details
CVE-2025-10791	A weakness has been identified in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/index.php. This manipulation of the argument aduser causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-10789	A vulnerability was identified in SourceCodester Online Hotel Reservation System 1.0. The impacted element is an unknown function of the file deleteslide.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10788	A vulnerability was determined in SourceCodester Online Hotel Reservation System 1.0. The affected element is an unknown function of the file deleteroominventory.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10596	A vulnerability was found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument usn results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10786	A flaw has been found in Campcodes Grocery Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_user. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-55912	An issue in ClipBucket 5.5.0 and prior versions allows an unauthenticated attacker can exploit the plupload endpoint in photo_uploader.php to upload arbitrary files without any authentication, due to missing access controls in the upload handler	7.3	More Details
CVE-2025-10687	A vulnerability was found in SourceCodester Responsive E-Learning System 1.0. This affects an unknown part of the file /admin/add_teacher.php. The manipulation of the argument Username results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-10688	A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file /admin/operation/paid.php. This manipulation of the argument inv_no/insta_amt causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-10623	A vulnerability was identified in SourceCodester Hotel Reservation System 1.0. The impacted element is an unknown function of the file deleteuser.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-53465	Deserialization of Untrusted Data vulnerability in raoinfotech GSheets Connector allows Object Injection. This issue affects GSheets Connector: from n/a through 1.1.1.	7.2	More Details
CVE-2025-58116	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in WN-7D36QR and WN-7D36QR/UE. If this vulnerability is exploited, an arbitrary OS command may be executed by a remote authenticated attacker.	7.2	More Details
CVE-2025-57919	Deserialization of Untrusted Data vulnerability in ConveyThis Language Translate Widget for WordPress – ConveyThis allows Object Injection. This issue affects Language Translate Widget for WordPress – ConveyThis: from n/a through 264.	7.2	More Details
CVE-2025-10207	Improper Validation of Specified Type of Input vulnerability in ABB FLXEON.This issue affects FLXEON: through 9.3.5.	7.2	More Details
CVE-2024-48851	Improper Validation of Specified Type of Input vulnerability in ABB FLXEON.A remote code execution is possible due to an improper input validation. This issue affects FLXEON: through 9.3.5.	7.2	More Details
CVE-2025-58662	Deserialization of Untrusted Data vulnerability in awesomesupport Awesome Support allows Object Injection. This issue affects Awesome Support: from n/a through 6.3.4.	7.2	More Details

CVE-2025-58259	Cross-Site Request Forgery (CSRF) vulnerability in scriptsbundle Nokri allows Cross Site Request Forgery. This issue affects Nokri: from n/a through 1.6.4.	7.1	More Details
CVE-2025-57968	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Reflected XSS. This issue affects VikRestaurants Table Reservations and Take-Away: from n/a through 1.4.	7.1	More Details
CVE-2025-57918	Cross-Site Request Forgery (CSRF) vulnerability in ERA404 LinkedInclude allows Stored XSS. This issue affects LinkedInclude: from n/a through 3.0.4.	7.1	More Details
CVE-2025-53692	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sitecore Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Cross-Site Scripting (XSS).This issue affects Sitecore Experience Manager (XM): from 9.2 through 10.4; Experience Platform (XP): from 9.2 through 10.4.	7.1	More Details
CVE-2025-58690	Cross-Site Request Forgery (CSRF) vulnerability in ptibogxiv Doliconnect allows Stored XSS. This issue affects Doliconnect: from n/a through 9.5.7.	7.1	More Details
CVE-2025-10456	A vulnerability was identified in the handling of Bluetooth Low Energy (BLE) fixed channels (such as SMP or ATT). Specifically, an attacker could exploit a flaw that causes the BLE target (i.e., the device under attack) to attempt to disconnect a fixed channel, which is not allowed per the Bluetooth specification. This leads to undefined behavior, including potential assertion failures, crashes, or memory corruption, depending on the BLE stack implementation.	7.1	More Details
CVE-2025-58261	Cross-Site Request Forgery (CSRF) vulnerability in PressPage Entertainment Inc Mavis HTTPS to HTTP Redirection allows Stored XSS. This issue affects Mavis HTTPS to HTTP Redirection: from n/a through 1.4.3.	7.1	More Details
CVE-2025-8411	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dokuzsoft Technology E-Commerce Web Design Product allows XSS Through HTTP Headers.This issue affects E-Commerce Web Design Product: before 11.08.2025.	7.1	More Details
CVE-2025-58262	Cross-Site Request Forgery (CSRF) vulnerability in wpdirectorykit Sweet Energy Efficiency allows Stored XSS. This issue affects Sweet Energy Efficiency: from n/a through 1.0.6.	7.1	More Details
CVE-2025-58688	Cross-Site Request Forgery (CSRF) vulnerability in Casengo Casengo Live Chat Support allows Stored XSS. This issue affects Casengo Live Chat Support: from n/a through 2.1.4.	7.1	More Details
CVE-2025-57977	Cross-Site Request Forgery (CSRF) vulnerability in wpdesk Flexible PDF Invoices for WooCommerce & WordPress allows Cross Site Request Forgery. This issue affects Flexible PDF Invoices for WooCommerce & WordPress: from n/a through 6.0.13.	7.1	More Details
CVE-2025-9969	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vizly Web Design Real Estate Packages allows Content Spoofing, CAPEC - 593 - Session Hijacking, CAPEC - 591 - Reflected XSS.This issue affects Real Estate Packages: before 5.1.	7.1	More Details
CVE-2025-58270	Cross-Site Request Forgery (CSRF) vulnerability in NIX Solutions Ltd NIX Anti-Spam Light allows Cross Site Request Forgery. This issue affects NIX Anti-Spam Light: from n/a through 0.0.4.	7.1	More Details
CVE-2025-58267	Cross-Site Request Forgery (CSRF) vulnerability in Aftabul Islam Stock Message allows Stored XSS. This issue affects Stock Message: from n/a through 1.1.0.	7.1	More Details
CVE-2025-58268	Cross-Site Request Forgery (CSRF) vulnerability in WPMK WPMK PDF Generator allows Stored XSS. This issue affects WPMK PDF Generator: from n/a through 1.0.1.	7.1	More Details
CVE-2025-58676	Cross-Site Request Forgery (CSRF) vulnerability in extendyourweb HORIZONTAL SLIDER allows Stored XSS. This issue affects HORIZONTAL SLIDER: from n/a through 2.4.	7.1	More Details
CVE-2025-58687	Cross-Site Request Forgery (CSRF) vulnerability in WP CMS Ninja Current Age Plugin allows Stored XSS. This issue affects Current Age Plugin: from n/a through 1.6.	7.1	More Details
CVE-2025-	Cross-Site Request Forgery (CSRF) vulnerability in loopus WP Attractive Donations System allows Stored XSS.	7.1	More

58956	This issue affects WP Attractive Donations System: from n/a through n/a.		Details
CVE-2025-58671	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in morganrichards Auction Feed allows Stored XSS. This issue affects Auction Feed: from n/a through 1.1.3.	7.1	More Details
CVE-2025-58670	Cross-Site Request Forgery (CSRF) vulnerability in Shankaranand Maurya WP Content Protection allows Stored XSS. This issue affects WP Content Protection: from n/a through 1.3.	7.1	More Details
CVE-2025-58677	Cross-Site Request Forgery (CSRF) vulnerability in puravida1976 ShrinkTheWeb (STW) Website Previews allows Stored XSS. This issue affects ShrinkTheWeb (STW) Website Previews: from n/a through 2.8.5.	7.1	More Details
CVE-2025-59335	CubeCart is an ecommerce software solution. Prior to version 6.5.11, there is an absence of automatic session expiration following a user's password change. This oversight poses a security risk, as if a user forgets to log out from a location where they accessed their account, an unauthorized user can maintain access even after the password has been changed. Due to this bug, if an account has already been compromised, the legitimate user has no way to revoke the attacker’s access. The malicious actor retains full access to the account until their session naturally expires. This means the account remains insecure even after the password has been changed. This issue has been patched in version 6.5.11.	7.1	More Details
CVE-2025-58657	Cross-Site Request Forgery (CSRF) vulnerability in EdwardBock Grid allows Stored XSS. This issue affects Grid: from n/a through 2.3.1.	7.1	More Details
CVE-2025-59215	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2024-48842	Use of Hard-coded Credentials vulnerability in ABB FLXEON.This issue affects FLXEON: through 9.3.5 and newer versions	7.0	More Details
CVE-2025-59216	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59220	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-0663	A cross-tenant authentication vulnerability exists in multiple WSO2 products due to improper cryptographic design in Adaptive Authentication. A single cryptographic key is used across all tenants to sign authentication cookies, allowing a privileged user in one tenant to forge authentication cookies for users in other tenants. Because the Auto-Login feature is enabled by default, this flaw may allow an attacker to gain unauthorized access and potentially take over accounts in other tenants. Successful exploitation requires access to Adaptive Authentication functionality, which is typically restricted to high-privileged users. The vulnerability is only exploitable when Auto-Login is enabled, reducing its practical impact in deployments where the feature is disabled.	6.8	More Details
CVE-2025-55038	An authorization bypass vulnerability has been discovered in the Click Plus C2-03CPU2 device firmware version 3.60. Through the KOPR protocol utilized by the Remote PLC application, authenticated users with low-level access permissions can exploit this vulnerability to read and modify PLC variables beyond their intended authorization level.	6.8	More Details
CVE-2025-59713	Snipe-IT before 8.1.18 allows unsafe deserialization.	6.8	More Details
CVE-2025-8531	Improper Handling of Length Parameter Inconsistency vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series Q03UDVCPU, Q04UDVCPU, Q06UDVCPU, Q13UDVCPU, Q26UDVCPU, Q04UDPVCPU, Q06UDPVCPU, Q13UDPVCPU, and Q26UDPVCPU with the first 5 digits of serial No. "24082" to "27081" allows a remote attacker to cause an integer underflow by sending specially crafted packets to the affected product to stop Ethernet communication and the execution of control programs on the product, when the user authentication function is enabled. The user authentication function is enabled by default only when settings are configured by GX Works2, which complies with the Cybersecurity Law of the People's Republic of China, and is normally disabled.	6.8	More Details
CVE-2025-57438	The 2wcom IP-4c 2.15.5 device suffers from a Broken Access Control vulnerability. Certain sensitive endpoints are intended to be accessible only after the admin explicitly grants access to a manager-level account. However, a manager-level user can bypass these controls by intercepting and modifying requests.	6.8	More Details

CVE-2025-9818	A vulnerability (CWE-428) has been identified in the Uninterruptible Power Supply (UPS) management application provided by OMRON SOCIAL SOLUTIONS Co., Ltd., where the executable file paths of Windows services are not enclosed in quotation marks. If the installation folder path of this product contains spaces, there is a possibility that unauthorized files may be executed under the service privileges by using paths containing spaces.	6.7	More Details
CVE-2025-23337	NVIDIA HGX & DGX GB200, GB300, B300 contain a vulnerability in the HGX Management Controller (HMC) that may allow a malicious actor with administrative access on the BMC to access the HMC as an administrator. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2025-54081	Sunshine is a self-hosted game stream host for Moonlight. Prior to version 2025.923.33222, the Windows service SunshineService is installed with an unquoted executable path. If Sunshine is installed in a directory whose name includes a space, the Service Control Manager (SCM) interprets the path incrementally and may execute a malicious binary placed earlier in the search string. This issue has been patched in version 2025.923.33222.	6.7	More Details
CVE-2025-26503	A crafted system call argument can cause memory corruption.	6.7	More Details
CVE-2025-5717	An authenticated remote code execution (RCE) vulnerability exists in multiple WSO2 products due to improper input validation in the event processor admin service. A user with administrative access to the SOAP admin services can exploit this flaw by deploying a Siddhi execution plan containing malicious Java code, resulting in arbitrary code execution on the server. Exploitation of this vulnerability requires a valid user account with administrative privileges, limiting the attack surface to authenticated but potentially malicious users.	6.7	More Details
CVE-2025-7937	There is a vulnerability in the Supermicro BMC firmware validation logic at Supermicro MBD-X12STW . An attacker can update the system firmware with a specially crafted image.	6.6	More Details
CVE-2025-10050	The Developer Loggers for Simple History plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 0.5 via the enabled_loggers parameter. This makes it possible for authenticated attackers, with Administrator-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.	6.6	More Details
CVE-2025-58237	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Niaj Morshed LC Wizard allows Stored XSS. This issue affects LC Wizard: from n/a through 1.3.0.	6.5	More Details
CVE-2025-58689	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tapfiliate Tapfiliate allows Stored XSS. This issue affects Tapfiliate: from n/a through 3.2.2.	6.5	More Details
CVE-2025-58648	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nicu Micle Simple JWT Login allows Stored XSS. This issue affects Simple JWT Login: from n/a through 3.6.4.	6.5	More Details
CVE-2025-53463	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HT Plugins HT Mega – Absolute Addons for WPBakery Page Builder allows DOM-Based XSS. This issue affects HT Mega – Absolute Addons for WPBakery Page Builder: from n/a through 1.0.9.	6.5	More Details
CVE-2025-53454	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Ultimate WP Mail allows Stored XSS. This issue affects Ultimate WP Mail: from n/a through 1.3.8.	6.5	More Details
CVE-2025-58651	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PlayerJS PlayerJS allows DOM-Based XSS. This issue affects PlayerJS: from n/a through 2.24.	6.5	More Details
CVE-2025-58652	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Carousel Ultimate allows Stored XSS. This issue affects Carousel Ultimate: from n/a through 1.8.	6.5	More Details
CVE-2025-58654	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-language allows DOM-Based XSS. This issue affects xili-language: from n/a through 2.21.3.	6.5	More Details
CVE-2025-	CubeCart is an ecommerce software solution. Prior to version 6.5.11, a logic flaw exists in the newsletter subscription endpoint that allows an attacker to unsubscribe any user without their consent. By changing the	6.5	More

59413	value of the force_unsubscribe parameter in the POST request to 1, an attacker can force the removal of any valid subscriber’s email address. This issue has been patched in version 6.5.11.		Details
CVE-2025-59347	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, The Manager disables TLS certificate verification in HTTP clients. The clients are not configurable, so users have no way to re-enable the verification. A Manager processes dozens of preheat jobs. An adversary performs a network-level Man-in-the-Middle attack, providing invalid data to the Manager. The Manager preheats with the wrong data, which later causes a denial of service and file integrity problems. This vulnerability is fixed in 2.1.0.	6.5	More Details
CVE-2025-57682	Directory Traversal vulnerability in Papermark 0.20.0 and prior allows authenticated attackers to retrieve arbitrary files from an S3 bucket through its CloudFront distribution via the "POST /api/file/s3/get-presigned-get-url-proxy" API	6.5	More Details
CVE-2025-57433	The 2wcom IP-4c 2.15.5 device's web interface includes an information disclosure vulnerability. By sending a crafted POST request to a specific endpoint (/cwi/ajax_request/get_data.php), an authenticated attacker (even with a low-privileged account like guest) can retrieve the hashed passwords for the admin, manager, and guest accounts. This significantly weakens the system's security posture, as these hashes could be cracked offline, granting attackers administrative access to the device.	6.5	More Details
CVE-2025-56648	npm parcel 2.0.0-alpha and before has an Origin Validation Error vulnerability. Malicious websites can send XMLHTTPRequests to the application's development server and read the response to steal source code when developers visit them.	6.5	More Details
CVE-2025-58678	Missing Authorization vulnerability in PickPlugins Accordion allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accordion: from n/a through 2.3.14.	6.5	More Details
CVE-2025-58680	Missing Authorization vulnerability in gutentor Gutentor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Gutentor: from n/a through 3.5.2.	6.5	More Details
CVE-2025-58682	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timur Kamaev Kama Click Counter allows Stored XSS. This issue affects Kama Click Counter: from n/a through 4.0.4.	6.5	More Details
CVE-2025-58683	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luke Mlsna Last Updated Shortcode allows Stored XSS. This issue affects Last Updated Shortcode: from n/a through 1.0.1.	6.5	More Details
CVE-2025-55911	An issue Clip Bucket v.5.5.2 Build#90 allows a remote attacker to execute arbitrary codes via the file_downloader.php and the file parameter	6.5	More Details
CVE-2025-53570	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DELUCKS DELUCKS SEO allows Stored XSS. This issue affects DELUCKS SEO: from n/a through 2.7.0.	6.5	More Details
CVE-2025-57898	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Vega WP Frontend Admin allows Stored XSS. This issue affects WP Frontend Admin: from n/a through 1.22.6.	6.5	More Details
CVE-2025-58264	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artbees JupiterX Core allows Stored XSS. This issue affects JupiterX Core: from n/a through 4.10.1.	6.5	More Details
CVE-2025-57948	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Directory Pro allows DOM-Based XSS. This issue affects Directory Pro: from n/a through 2.5.5.	6.5	More Details
CVE-2025-57947	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Photo Gallery by Ays allows DOM-Based XSS. This issue affects Photo Gallery by Ays: from n/a through 6.3.6.	6.5	More Details
CVE-2025-57938	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themewant Easy Hotel Booking allows DOM-Based XSS. This issue affects Easy Hotel Booking: from n/a through 1.6.9.	6.5	More Details
CVE-2025-57932	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Diego Pereira PowerFolio allows Stored XSS. This issue affects PowerFolio: from n/a through 3.2.1.	6.5	More Details
CVE-			

2025-57926	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Passster allows Stored XSS. This issue affects Passster: from n/a through 4.2.18.	6.5	More Details
CVE-2025-58263	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev BuddyPress Notification Widget allows Stored XSS. This issue affects BuddyPress Notification Widget: from n/a through 1.3.3.	6.5	More Details
CVE-2025-58265	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stonehenge Creations Events Manager – OpenStreetMaps allows Stored XSS. This issue affects Events Manager – OpenStreetMaps: from n/a through 4.2.1.	6.5	More Details
CVE-2025-57900	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ataur R GutenKit allows Stored XSS. This issue affects GutenKit: from n/a through 2.4.2.	6.5	More Details
CVE-2025-57913	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eleopard Behance Portfolio Manager allows Stored XSS. This issue affects Behance Portfolio Manager: from n/a through 1.7.4.	6.5	More Details
CVE-2025-57911	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Adverts allows DOM-Based XSS. This issue affects Adverts: from n/a through 1.4.	6.5	More Details
CVE-2025-57910	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AnyClip Video Platform AnyClip Luminous Studio allows Stored XSS. This issue affects AnyClip Luminous Studio: from n/a through 1.3.3.	6.5	More Details
CVE-2025-57909	Missing Authorization vulnerability in Rouergue Création Editor Custom Color Palette allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Editor Custom Color Palette: from n/a through 3.4.8.	6.5	More Details
CVE-2025-57902	Cross-Site Request Forgery (CSRF) vulnerability in Md Taufiqur Rahman RIS Version Switcher – Downgrade or Upgrade WP Versions Easily allows Cross Site Request Forgery. This issue affects RIS Version Switcher – Downgrade or Upgrade WP Versions Easily: from n/a through 1.0.	6.5	More Details
CVE-2025-57901	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DAEXT Import Markdown allows Stored XSS. This issue affects Import Markdown: from n/a through 1.14.	6.5	More Details
CVE-2025-58684	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Logo Showcase allows Stored XSS. This issue affects Logo Showcase: from n/a through 3.0.9.	6.5	More Details
CVE-2025-58691	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson Genesis Club Lite allows Stored XSS. This issue affects Genesis Club Lite: from n/a through 1.17.	6.5	More Details
CVE-2025-57954	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Poll Maker allows DOM-Based XSS. This issue affects Poll Maker: from n/a through 6.0.1.	6.5	More Details
CVE-2025-58702	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebWizards MarketKing allows Stored XSS. This issue affects MarketKing: from n/a through 2.0.92.	6.5	More Details
CVE-2025-59586	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Portfolio allows DOM-Based XSS. This issue affects Penci Portfolio: from n/a through 3.5.	6.5	More Details
CVE-2025-59587	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Shortcodes & Performance allows DOM-Based XSS. This issue affects Penci Shortcodes & Performance: from n/a through n/a.	6.5	More Details
CVE-2025-59589	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Soledad allows DOM-Based XSS. This issue affects Soledad: from n/a through 8.6.8.	6.5	More Details
CVE-2025-59592	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fernando Acosta Make Column Clickable Elementor allows Stored XSS. This issue affects Make Column Clickable Elementor: from n/a through 1.6.0.	6.5	More Details
CVE-2025-	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, arbitrary themes can be loaded through query parameters. If an installed	6.5	More

59535	theme had a vulnerability, even if it was not used on any page, this could be loaded on unsuspecting clients without knowledge of the site owner. This issue has been patched in version 10.1.0.		Details
CVE-2025-58915	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emarket-design YouTube Showcase youtube-showcase allows Stored XSS.This issue affects YouTube Showcase: from n/a through 3.5.0.	6.5	More Details
CVE-2025-59714	In Internet2 Grouper 5.17.1 before 5.20.5, group admins who are not Grouper sysadmins can configure loader jobs.	6.5	More Details
CVE-2025-10548	The CleverControl employee monitoring software (v11.5.1041.6) fails to validate TLS server certificates during the installation process. The installer downloads and executes external components using curl.exe --insecure, enabling a man-in-the-middle attacker to deliver malicious files that are executed with SYSTEM privileges. This can lead to full remote code execution with administrative rights. No patch is available as the vendor has been unresponsive. It is assumed that previous versions are also affected, but this is not confirmed.	6.5	More Details
CVE-2025-9342	Authorization Bypass Through User-Controlled Key vulnerability in Anadolu Hayat Emeklilik Inc. AHE Mobile allows Privilege Abuse.This issue affects AHE Mobile: from 1.9.7 before 1.9.9.	6.5	More Details
CVE-2024-4598	An information disclosure vulnerability exists in multiple WSO2 products due to improper implementation of the enrich mediator. Authenticated users may be able to view unintended business data from other mediation contexts because the internal state is not properly isolated or cleared between executions. This vulnerability does not impact user credentials or access tokens but may lead to leakage of sensitive business information handled during message flows.	6.5	More Details
CVE-2025-59821	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, DNN's URL/path handling and template rendering can allow specially crafted input to be reflected into a user profile that is returned to the browser. In these cases, the application does not sufficiently neutralize or encode characters that are meaningful in HTML, so an attacker can cause a victim's browser to interpret attacker-controlled content as part of the page's HTML. This issue has been patched in version 10.1.0.	6.5	More Details
CVE-2025-9215	The StoreEngine – Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.0 via the file_download() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-10658	The SupportCandy – Helpdesk & Customer Support Ticket System plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 3.3.7. This is due to missing rate limiting on the OTP verification for guest login. This makes it possible for unauthenticated attackers to bypass authentication and gain unauthorized access to customer support tickets by brute forcing the 6-digit OTP code.	6.5	More Details
CVE-2025-10652	The Robcore Netatmo plugin for WordPress is vulnerable to SQL Injection via the 'module_id' attribute of the robcore-netatmo shortcode in all versions up to, and including, 1.7 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 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-2025-57396	Tandoor Recipes 2.0.0-alpha-1, fixed in 2.0.0-alpha-2, is vulnerable to privilege escalation. This is due to the rework of the API, which resulted in the User Profile API Endpoint containing two boolean values indicating whether a user is staff or administrative. Consequently, any user can escalate their privileges to the highest level.	6.5	More Details
CVE-2025-59585	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Recipe allows DOM-Based XSS. This issue affects Penci Recipe: from n/a through 4.0.	6.5	More Details
CVE-2025-59584	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Podcast allows DOM-Based XSS. This issue affects Penci Podcast: from n/a through 1.6.	6.5	More Details
CVE-2025-59583	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Filter Everything allows DOM-Based XSS. This issue affects Penci Filter Everything: from n/a through n/a.	6.5	More Details
CVE-2025-59549	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fatcatapps GetResponse Forms allows Stored XSS. This issue affects GetResponse Forms: from n/a through 2.6.0.	6.5	More Details
CVE-			

2025-58703	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skyword Skyword API Plugin allows Stored XSS. This issue affects Skyword API Plugin: from n/a through 2.5.3.	6.5	More Details
CVE-2025-57055	WonderCMS 3.5.0 is vulnerable to Server-Side Request Forgery (SSRF) in the custom module installation functionality. An authenticated administrator can supply a malicious URL via the pluginThemeUrl POST parameter. The server fetches the provided URL using curl_exec() without sufficient validation, allowing the attacker to force internal or external HTTP requests.	6.5	More Details
CVE-2025-58704	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ren Ventura WP Delete User Accounts allows Stored XSS. This issue affects WP Delete User Accounts: from n/a through 1.2.4.	6.5	More Details
CVE-2025-58965	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Agency Dominion Inc. Fusion Page Builder : Extension – Gallery allows Stored XSS. This issue affects Fusion Page Builder : Extension – Gallery: from n/a through 1.7.6.	6.5	More Details
CVE-2025-58974	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StellarWP WPComplete allows Stored XSS. This issue affects WPComplete: from n/a through 2.9.5.2.	6.5	More Details
CVE-2025-58992	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode Product Catalog Simple allows Stored XSS. This issue affects Product Catalog Simple: from n/a through 1.8.2.	6.5	More Details
CVE-2025-59552	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pdfcrowd Dev Team Save as PDF allows Stored XSS. This issue affects Save as PDF: from n/a through 4.5.2.	6.5	More Details
CVE-2025-59581	Missing Authorization vulnerability in VW THEMES Ibtana allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ibtana: from n/a through 1.2.5.3.	6.5	More Details
CVE-2025-47906	If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.	6.5	More Details
CVE-2025-59553	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Coderz Studio Custom iFrame for Elementor allows DOM-Based XSS. This issue affects Custom iFrame for Elementor: from n/a through 1.0.13.	6.5	More Details
CVE-2025-59565	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Swings Upsell Order Bump Offer for WooCommerce allows Stored XSS. This issue affects Upsell Order Bump Offer for WooCommerce: from n/a through 3.0.7.	6.5	More Details
CVE-2025-59569	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emraan Cheema CubeWP allows Stored XSS. This issue affects CubeWP: from n/a through 1.1.26.	6.5	More Details
CVE-2025-59574	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Travel Engine WP Travel Engine allows Stored XSS. This issue affects WP Travel Engine: from n/a through 1.4.2.	6.5	More Details
CVE-2025-59576	Missing Authorization vulnerability in Stylemix MasterStudy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MasterStudy LMS: from n/a through 3.6.20.	6.5	More Details
CVE-2025-57953	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 100plugins Open User Map allows DOM-Based XSS. This issue affects Open User Map: from n/a through 1.4.14.	6.5	More Details
CVE-2025-58653	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JS Morisset JSM file_get_contents() Shortcode allows Stored XSS. This issue affects JSM file_get_contents() Shortcode: from n/a through 2.7.1.	6.5	More Details
CVE-2025-57955	Missing Authorization vulnerability in Plugin Devs Post Carousel Slider for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Post Carousel Slider for Elementor: from n/a through 1.7.0.	6.5	More Details
CVE-2025-58020	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress allows Stored XSS. This issue affects Theater for WordPress: from n/a through 0.18.8.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aum		More

2025-58028	Watcharapon Designil PDPA Thailand allows Stored XSS. This issue affects Designil PDPA Thailand: from n/a through 2.0.	6.5	Details
CVE-2025-58027	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpo-HR NGG Smart Image Search allows Stored XSS. This issue affects NGG Smart Image Search: from n/a through 3.4.3.	6.5	More Details
CVE-2025-58026	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in termageddon Termageddon: Cookie Consent & Privacy Compliance allows Stored XSS. This issue affects Termageddon: Cookie Consent & Privacy Compliance: from n/a through 1.8.1.	6.5	More Details
CVE-2025-58025	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in averta Master Slider allows Stored XSS. This issue affects Master Slider: from n/a through 3.11.0.	6.5	More Details
CVE-2025-58023	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in akdevs Genealogical Tree allows Stored XSS. This issue affects Genealogical Tree: from n/a through 2.2.5.	6.5	More Details
CVE-2025-58022	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in maxpagels ShortCode allows Stored XSS. This issue affects ShortCode: from n/a through 0.8.1.	6.5	More Details
CVE-2025-58021	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in douglaskarr List Child Pages Shortcode allows Stored XSS. This issue affects List Child Pages Shortcode: from n/a through 1.3.1.	6.5	More Details
CVE-2025-58019	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Search Atlas Search Atlas SEO allows Stored XSS. This issue affects Search Atlas SEO: from n/a through 2.5.4.	6.5	More Details
CVE-2025-58031	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nextendweb Nextend Facebook Connect allows Stored XSS. This issue affects Nextend Facebook Connect : from n/a through 3.1.19.	6.5	More Details
CVE-2025-58018	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Richard Leishman Mail Subscribe List allows Stored XSS. This issue affects Mail Subscribe List: from n/a through 2.1.10.	6.5	More Details
CVE-2025-58017	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes Ultimate Store Kit Elementor Addons allows Stored XSS. This issue affects Ultimate Store Kit Elementor Addons: from n/a through 2.8.2.	6.5	More Details
CVE-2025-58008	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xnau webdesign Participants Database allows Stored XSS. This issue affects Participants Database: from n/a through 2.7.6.3.	6.5	More Details
CVE-2025-58002	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Milan Petrovic GD bbPress Tools allows DOM-Based XSS. This issue affects GD bbPress Tools: from n/a through 3.5.3.	6.5	More Details
CVE-2025-58001	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noumaan Yaqoob Compact Archives allows Stored XSS. This issue affects Compact Archives: from n/a through 4.1.0.	6.5	More Details
CVE-2025-57999	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpkoithemes WPKoi Templates for Elementor allows DOM-Based XSS. This issue affects WPKoi Templates for Elementor: from n/a through 3.4.1.	6.5	More Details
CVE-2025-57996	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matthewordie Buckets allows Stored XSS. This issue affects Buckets: from n/a through 0.3.9.	6.5	More Details
CVE-2025-58030	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Page-list allows Stored XSS. This issue affects Page-list: from n/a through 5.7.	6.5	More Details
CVE-2025-58254	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dtbaker StylePress for Elementor allows Stored XSS. This issue affects StylePress for Elementor: from n/a through 1.2.1.	6.5	More Details
CVE-2025-57989	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brajesh Singh WordPress Widgets Shortcode allows Stored XSS. This issue affects WordPress Widgets Shortcode: from n/a through 1.0.3.	6.5	More Details

CVE-2025-58231	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bitlydeveloper Bitly allows Stored XSS. This issue affects Bitly: from n/a through 2.7.4.	6.5	More Details
CVE-2025-58238	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ONTRAPORT PilotPress allows Stored XSS. This issue affects PilotPress: from n/a through 2.0.35.	6.5	More Details
CVE-2025-58235	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Front End Users allows Stored XSS. This issue affects Front End Users: from n/a through 3.2.33.	6.5	More Details
CVE-2025-58234	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JoomSky JS Job Manager allows Stored XSS. This issue affects JS Job Manager: from n/a through 2.0.2.	6.5	More Details
CVE-2025-58233	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Guaven Labs SQL Chart Builder allows DOM-Based XSS. This issue affects SQL Chart Builder: from n/a through 2.3.7.2.	6.5	More Details
CVE-2025-58239	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chandrika Sista WP Category Dropdown allows Stored XSS. This issue affects WP Category Dropdown: from n/a through 1.9.	6.5	More Details
CVE-2025-58240	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-tidy-tags allows Stored XSS. This issue affects xili-tidy-tags: from n/a through 1.12.06.	6.5	More Details
CVE-2025-58232	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ickata Image Editor by Pixo allows DOM-Based XSS. This issue affects Image Editor by Pixo: from n/a through 2.3.8.	6.5	More Details
CVE-2025-58230	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes ZoloBlocks allows DOM-Based XSS. This issue affects ZoloBlocks: from n/a through 2.3.9.	6.5	More Details
CVE-2025-58220	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Techeshta Card Elements for WPBakery allows DOM-Based XSS. This issue affects Card Elements for WPBakery: from n/a through 1.0.8.	6.5	More Details
CVE-2025-58229	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Sitekit allows Stored XSS. This issue affects Sitekit: from n/a through 2.0.	6.5	More Details
CVE-2025-58241	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snapwidget SnapWidget Social Photo Feed Widget allows DOM-Based XSS. This issue affects SnapWidget Social Photo Feed Widget: from n/a through 1.1.0.	6.5	More Details
CVE-2025-58228	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC Quick View for WooCommerce allows Stored XSS. This issue affects Quick View for WooCommerce: from n/a through 2.2.16.	6.5	More Details
CVE-2025-58242	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vadim Bogaiskov Bg Church Memos allows DOM-Based XSS. This issue affects Bg Church Memos: from n/a through 1.1.	6.5	More Details
CVE-2025-58227	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexander Lueken Podlove Subscribe button allows Stored XSS. This issue affects Podlove Subscribe button: from n/a through 1.3.11.	6.5	More Details
CVE-2025-58248	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codefish Pinterest Pinboard Widget allows Stored XSS. This issue affects Pinterest Pinboard Widget: from n/a through 1.0.7.	6.5	More Details
CVE-2025-58253	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rameez Iqbal Real Estate Manager allows DOM-Based XSS. This issue affects Real Estate Manager: from n/a through 7.3.	6.5	More Details
CVE-2025-57993	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Pick Geolocation IP Detection allows Stored XSS. This issue affects Geolocation IP Detection: from n/a through 5.5.0.	6.5	More Details
	Tenda AC6 router firmware 15.03.05.19 contains a command injection vulnerability in the formSetIptv		

CVE-2025-57296	function, which processes requests to the /goform/SetIPTVCfg web interface. When handling the list and vlanId parameters, the sub_ADBC0 helper function concatenates these user-supplied values into nvram set system commands using doSystemCmd, without validating or sanitizing special characters (e.g., ;, ", #). An unauthenticated or authenticated attacker can exploit this by submitting a crafted POST request, leading to arbitrary system command execution on the affected device.	6.5	More Details
CVE-2025-57983	Cross-Site Request Forgery (CSRF) vulnerability in Damian BP Disable Activation Reloaded allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects BP Disable Activation Reloaded: from n/a through 1.2.1.	6.5	More Details
CVE-2025-57986	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in husani WP Subtitle allows Stored XSS. This issue affects WP Subtitle: from n/a through 3.4.1.	6.5	More Details
CVE-2025-57981	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catchsquare WP Social Widget allows Stored XSS. This issue affects WP Social Widget: from n/a through 2.3.1.	6.5	More Details
CVE-2025-57988	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash allows Stored XSS. This issue affects Uncanny Toolkit for LearnDash: from n/a through 3.0.7.3.	6.5	More Details
CVE-2025-57967	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Quick View for WooCommerce allows Stored XSS. This issue affects WPB Quick View for WooCommerce: from n/a through 2.1.8.	6.5	More Details
CVE-2025-58260	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ronald Huereca Highlight and Share – Social Text and Image Sharing allows Stored XSS. This issue affects Highlight and Share – Social Text and Image Sharing: from n/a through 5.1.1.	6.5	More Details
CVE-2025-57966	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Gallery Lightbox allows Stored XSS. This issue affects Gallery Lightbox: from n/a through 1.0.0.41.	6.5	More Details
CVE-2025-58257	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Picture-Planet GmbH Verowa Connect allows Stored XSS. This issue affects Verowa Connect: from n/a through 3.2.3.	6.5	More Details
CVE-2025-57965	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CodeUs WP Proposals allows Stored XSS. This issue affects WP Proposals: from n/a through 2.3.	6.5	More Details
CVE-2025-57963	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoho Subscriptions Zoho Billing allows DOM-Based XSS. This issue affects Zoho Billing: from n/a through 4.1.	6.5	More Details
CVE-2025-57964	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in photonicgnostic Library Bookshelves allows Stored XSS. This issue affects Library Bookshelves: from n/a through 5.11.	6.5	More Details
CVE-2025-58962	Server-Side Request Forgery (SSRF) vulnerability in publitio Publitio allows Server Side Request Forgery. This issue affects Publitio: from n/a through 2.2.1.	6.4	More Details
CVE-2025-59712	Snipe-IT before 8.1.18 allows XSS.	6.4	More Details
CVE-2025-8902	The Widget Options - Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'do_sidebar' shortcode in all versions up to, and including, 5.2.1 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-2025-58011	Server-Side Request Forgery (SSRF) vulnerability in Alex Content Mask allows Server Side Request Forgery. This issue affects Content Mask: from n/a through 1.8.5.2.	6.4	More Details
CVE-2025-6198	There is a vulnerability in the Supermicro BMC firmware validation logic at Supermicro MBD-X13SEM-F . An attacker can update the system firmware with a specially crafted image.	6.4	More Details
	The Ghost Kit – Page Builder Blocks, Motion Effects & Extensions plugin for WordPress is vulnerable to Stored		

CVE-2025-9992	Cross-Site Scripting via the custom JS field in all versions up to, and including, 3.4.3 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-2025-9565	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocksy_newsletter_subscribe shortcode in all versions up to, and including, 2.1.10 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-2025-10166	The Social Media Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'twitter' shortcode in all versions up to, and including, 1.3.1 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-2025-26514	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a Reflected Cross-Site Scripting vulnerability. Successful exploit could allow an attacker to view or modify configuration settings or add or modify user accounts but requires the attacker to know specific information about the target instance and then trick a privileged user into clicking a specially crafted link.	6.4	More Details
CVE-2025-8394	The Productive Style plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's display_productive_breadcrumb shortcode in all versions up to, and including, 1.1.23 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-2025-48007	Improper Encoding or Escaping of Output vulnerability in Hallo Welt! GmbH BlueSpice (Extension:BlueSpiceAvatars) allows Cross-Site Scripting (XSS). This issue affects BlueSpice: from 5 through 5.1.1.	6.4	More Details
CVE-2025-10181	The Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'drafts' shortcode in all versions up to, and including, 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-2025-9851	The Appointmind plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'appointmind_calendar' shortcode in all versions up to, and including, 4.1.0 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-2025-9203	The Media Player Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subtitle_ssize', 'track_title', and 'track_artist_name' parameters in version 1.0.5. This is 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-2025-46703	Improper Encoding or Escaping of Output vulnerability in Hallo Welt! GmbH BlueSpice (Extension:AtMentions) allows Cross-Site Scripting (XSS). This issue affects BlueSpice: from 5 through 5.1.1.	6.4	More Details
CVE-2025-8532	Authorization Bypass Through User-Controlled Key, CWE - 862 - Missing Authorization, – Improper Authorization vulnerability in Bimser Solution Software Trade Inc. EBA Document and Workflow Management System allows – Exploitation of Trusted Identifiers, – Exploitation of Authorization, – Variable Manipulation.This issue affects eBA Document and Workflow Management System: from 6.7.164 before 6.7.166.	6.4	More Details
CVE-2025-10125	The Memberlite Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugins's 'row' shortcode in all versions up to, and including, 1.4 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-2025-10771	A vulnerability was determined in jeecgboot JimuReport up to 2.1.2. Affected is an unknown function of the file /drag/onlDragDataSource/testConnection of the component DB2 JDBC Handler. Executing manipulation of the argument clientRerouteServerListJNDIName can lead to deserialization. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-	A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. The impacted element is an unknown function of the file /admin/inv-print.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the	6.3	More Details

10839	public and may be exploited.		
CVE-2025-10770	A vulnerability was found in jeecgboot JimuReport up to 2.1.2. This impacts an unknown function of the file /drag/onlDragDataSource/testConnection of the component MySQL JDBC Handler. Performing manipulation results in deserialization. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10777	A flaw has been found in JSC R7 R7-Office Document Server up to 20250820. Impacted is an unknown function of the file /downloadas/. Executing manipulation of the argument cmd can lead to path traversal. The attack can be launched remotely. Upgrading to version 2025.3.1.923 is recommended to address this issue. The affected component should be upgraded. R7-Office is a fork of OpenOffice and at the moment it remains unclear if OpenOffice is affected as well. The OpenOffice team was not able to reproduce the issue in their codebase. The vendor replied: "We confirm that this vulnerability has been verified and patched in release 2025.3.1.923. During our security testing, it was not possible to exploit the issue - the server consistently returns proper error responses to the provided scenarios."	6.3	More Details
CVE-2025-10772	A vulnerability was identified in huggingface LeRobot up to 0.3.3. Affected by this vulnerability is an unknown functionality of the file lerobot/common/robot_devices/robots/lekiwi_remote.py of the component ZeroMQ Socket Handler. The manipulation leads to missing authentication. The attack can only be initiated within the local network. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10835	A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. This impacts an unknown function of the file /admin/view_payorder.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10780	A vulnerability was determined in CodeAstro Simple Pharmacy Management 1.0. This affects an unknown function of the file /view.php. This manipulation of the argument bar_code causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-10828	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown part of the file /admin/edit.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-10826	A security flaw has been discovered in Campcodes Online Beauty Parlor Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/sales-reports-detail.php. The manipulation of the argument fromdate/todate results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10840	A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown function of the file /admin/print-payment.php. This manipulation of the argument sql111 causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-10814	A vulnerability was determined in D-Link DIR-823X 240126/240802/250416. Affected by this vulnerability is an unknown functionality of the file /usr/sbin/goahead. This manipulation of the argument port causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-10825	A vulnerability was identified in Campcodes Online Beauty Parlor Management System 1.0. Affected is an unknown function of the file /admin/view-appointment.php. The manipulation of the argument viewid leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-10763	A vulnerability was determined in academico-sis academico up to d9a9e2636fbf7e5845ee086bcb03ca62faceb6ab. Affected by this issue is some unknown functionality of the file /edit-photo of the component Profile Picture Handler. This manipulation causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. This product adopts a rolling release strategy to maintain continuous delivery The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10634	A weakness has been identified in D-Link DIR-823X 240126/240802/250416. The impacted element is the function sub_412E7C of the file /usr/sbin/goahead of the component Environment Variable Handler. This manipulation of the argument terminal_addr/server_ip/server_port causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-10769	A vulnerability has been found in h2oai h2o-3 up to 3.46.08. This affects an unknown function of the file /99/ImportSQLTable of the component H2 JDBC Driver. Such manipulation of the argument connection_url leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-	A vulnerability was detected in SourceCodester Online Exam Form Submission 1.0. Affected by this vulnerability is an unknown functionality of the file /user/dashboard.php?page=update_profile. The		More

2025-10625	manipulation of the argument phone results in sql injection. The attack may be launched remotely. The exploit is now public and may be used. Other parameters might be affected as well.	6.3	Details
CVE-2025-8664	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saysis Computer Systems Trade Ltd. Co. StarCities E-Municipality Management allows Cross-Site Scripting (XSS).This issue affects StarCities E-Municipality Management: before 20250825.	6.3	More Details
CVE-2025-10626	A flaw has been found in SourceCodester Online Exam Form Submission 1.0. Affected by this issue is some unknown functionality of the file /admin/update_s3.php. This manipulation of the argument credits causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2025-10627	A vulnerability has been found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /admin/delete_user.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-10741	A security vulnerability has been detected in Selleo Mentingo up to 2025.08.27. The affected element is an unknown function of the component Profile Picture Handler. The manipulation of the argument userAvatar leads to unrestricted upload. The attack is possible to be carried out 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-2025-10755	A vulnerability was detected in Selleo Mentingo 2025.08.27. The impacted element is an unknown function of the component Content-Type Handler. The manipulation of the argument userAvatar results in unrestricted upload. The attack may be performed from remote. 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-2025-10628	A vulnerability was found in D-Link DIR-852 1.00CN B09. This vulnerability affects unknown code of the file /htdocs/cgibin/hedwig.cgi of the component Web Management Interface. Performing manipulation results in command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-59539	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, when embedding information in the Biography field, even if that field is not rich-text, users could inject javascript code that would run in the context of the website and to any other user that can view the profile including administrators and/or superusers. This issue has been patched in version 10.1.0.	6.3	More Details
CVE-2025-10707	A weakness has been identified in JeecgBoot up to 3.8.2. Affected is an unknown function of the file /message/sysMessageTemplate/sendMsg. Executing manipulation can lead to improper authorization. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10629	A vulnerability was determined in D-Link DIR-852 1.00CN B09. This issue affects the function ssdpcgi_main of the file htodcs/cgibin of the component Simple Service Discovery Protocol Service. Executing manipulation of the argument ST can lead to command injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-10760	A flaw has been found in Harness 3.3.0. This impacts the function LookupRepo of the file app/api/controller/gitspace/lookup_repo.go. Executing manipulation of the argument url can lead to server-side request forgery. The attack may 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-2025-10592	A security vulnerability has been detected in itsourcecode Online Public Access Catalog OPAC 1.0. This impacts an unknown function of the file mysearch.php of the component POST Parameter Handler. Such manipulation of the argument search_field/search_text leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-10848	A vulnerability was identified in Campcodes Society Membership Information System 1.0. This issue affects some unknown processing of the file /check_student.php. Such manipulation of the argument student_id leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-10846	A vulnerability was determined in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /module/ComponenteCurricular/edit. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-10593	A vulnerability was detected in SourceCodester Online Student File Management System 1.0. Affected is an unknown function of the file /admin/update_student.php. Performing manipulation of the argument stud_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details

CVE-2025-10762	A vulnerability was found in kuaifan DooTask up to 1.2.49. Affected by this vulnerability is an unknown functionality of the file app/Http/Controllers/Api/UsersController.php. The manipulation of the argument keys[department] results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10594	A flaw has been found in SourceCodester Online Student File Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/delete_student.php. Executing manipulation of the argument stud_id can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-10845	A vulnerability was found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /module/ComponenteCurricular/view. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10844	A vulnerability has been found in Portabilis i-Educar up to 2.10. Affected by this issue is some unknown functionality of the file /module/Cadastro/aluno. The manipulation of the argument is leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-10764	A vulnerability was identified in SeriaWei ZKEACMS up to 4.3. This affects the function Edit of the file src/ZKEACMS.EventAction/Controllers/PendingTaskController.cs of the component Event Action System. Such manipulation of the argument Data leads to server-side request forgery. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10768	A flaw has been found in h2oai h2o-3 up to 3.46.08. The impacted element is an unknown function of the file /99/ImportSQLTable of the component IBMDB2 JDBC Driver. This manipulation of the argument connection_url causes deserialization. The attack may 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-2025-10689	A vulnerability was identified in D-Link DIR-645 105B01. This issue affects the function soapcgi_main of the file /soap.cgi. Such manipulation of the argument service leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-54390	A Cross-Site Request Forgery (CSRF) vulnerability exists in the ResetPasswordRequest operation of Zimbra Collaboration (ZCS) when the zimbraFeatureResetPasswordStatus attribute is enabled. An attacker can exploit this by tricking an authenticated user into visiting a malicious webpage that silently sends a crafted SOAP request to reset the user's password. The vulnerability stems from a lack of CSRF token validation on the endpoint, allowing password resets without the user's consent.	6.3	More Details
CVE-2025-10665	A vulnerability was identified in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. Affected is an unknown function of the file /Profilers/PProfile/COUNT3s3.php. The manipulation of the argument csem leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	6.3	More Details
CVE-2025-10807	A security flaw has been discovered in Campcodes Online Beauty Parlor Management System 1.0. This issue affects some unknown processing of the file /admin/edit-customer-detailed.php. The manipulation of the argument editid results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10602	A vulnerability was found in SourceCodester Online Exam Form Submission 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/delete_s1.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10608	A vulnerability was detected in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /enrollment-history/. Performing manipulation results in improper access controls. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-10804	A vulnerability was found in Campcodes Online Beauty Parlor Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/add-customer.php. Performing manipulation of the argument mobilenum results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10805	A vulnerability was determined in Campcodes Online Beauty Parlor Management System 1.0. This affects an unknown part of the file /admin/add-services.php. Executing manipulation of the argument sername can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-	A vulnerability has been found in itsourcecode Student Information System 1.0. The affected element is an		

2025-10613	unknown function of the file /leveledit1.php. Such manipulation of the argument level_id leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-10806	A vulnerability was identified in Campcodes Online Beauty Parlor Management System 1.0. This vulnerability affects unknown code of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-10616	A security flaw has been discovered in itsourcecode E-Commerce Website 1.0. Affected is an unknown function of the file /admin/users.php. The manipulation results in unrestricted upload. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10595	A vulnerability has been found in SourceCodester Online Student File Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/delete_user.php. The manipulation of the argument user_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-55885	SQL Injection vulnerability in Alpes Recherche et Developpement ARD GEC en Lign before v.2025-04-23 allows a remote attacker to escalate privileges via the GET parameters in index.php	6.3	More Details
CVE-2025-10617	A weakness has been identified in SourceCodester Online Polling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/positions.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-10618	A security vulnerability has been detected in itsourcecode Online Clinic Management System 1.0. Affected by this issue is some unknown functionality of the file transact.php. Such manipulation of the argument firstname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. Other parameters might be affected as well.	6.3	More Details
CVE-2025-10619	A vulnerability was detected in sequa-ai sequa-mcp up to 1.0.13. This affects the function redirectToAuthorization of the file src/helpers/node-oauth-client-provider.ts of the component OAuth Server Discovery. Performing manipulation results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. Upgrading to version 1.0.14 is able to mitigate this issue. The patch is named e569815854166db5f71c2e722408f8957fb9e804. It is recommended to upgrade the affected component. The vendor explains: "We only promote that mcp server with our own URLs that have a valid response, but yes if someone would use it with a non sequa url, this is a valid attack vector. We have released a new version (1.0.14) that fixes this and validates that only URLs can be opened."	6.3	More Details
CVE-2025-10669	A vulnerability was detected in Airsonic-Advanced up to 10.6.0. This vulnerability affects unknown code of the component Playlist Upload Handler. Performing manipulation results in unrestricted upload. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-10620	A flaw has been found in itsourcecode Online Clinic Management System 1.0. This vulnerability affects unknown code of the file /editp2.php. Executing manipulation of the argument id/firstname/lastname/type/age/address can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-10790	A security flaw has been discovered in SourceCodester Simple Forum Discussion System 1.0. This affects an unknown function of the file /ajax.php?action=save_category. The manipulation of the argument Description results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-10615	A vulnerability was identified in itsourcecode E-Commerce Website 1.0. This impacts an unknown function of the file /admin/products.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-55910	CMSEasy v7.7.8.0 and before is vulnerable to Arbitrary file deletion in database_admin.php.	6.3	More Details
CVE-2025-10787	A vulnerability was found in MuYuCMS up to 2.7. Impacted is an unknown function of the file /index/index.html of the component Add Fiend Link Handler. Performing manipulation of the argument Link URL results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-58431	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.4.1 and earlier, the /v2_1/files/file/download endpoint allows file read from ANY USER who has access to localhost. File reads are performed AS ROOT.	6.2	More Details
CVE-			

2025-8282	The SureForms WordPress plugin before 1.9.1 does not sanitise and escape some parameters when outputing them in the page, which could allow admin and above users to perform Cross-Site Scripting attacks.	6.1	More Details
CVE-2025-59689	Libraesva ESG 4.5 through 5.5.x before 5.5.7 allows command injection via a compressed e-mail attachment. For ESG 5.0 a fix has been released in 5.0.31. For ESG 5.1 a fix has been released in 5.1.20. For ESG 5.2 a fix has been released in 5.2.31. For ESG 5.4 a fix has been released in 5.4.8. For ESG 5.5. a fix has been released in 5.5.7.	6.1	More Details
CVE-2025-9883	The Browser Sniff plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-37122	A vulnerability in the web-based management interface of network access control services could allow an unauthenticated remote attacker to conduct a Reflected Cross-Site Scripting (XSS) attack. Successful exploitation could allow an attacker to execute arbitrary JavaScript code in a victim's browser in the context of the affected interface.	6.1	More Details
CVE-2025-9882	The osTicket WP Bridge plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.2. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-10146	The Download Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘user_ids’ parameter in all versions up to, and including, 3.3.23 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-0209	A reflected cross-site scripting (XSS) vulnerability exists in the account registration flow of WSO2 Identity Server due to improper output encoding. A malicious actor can exploit this vulnerability by injecting a crafted payload that is reflected in the server response, enabling the execution of arbitrary JavaScript in the victim's browser. This vulnerability could allow attackers to redirect users to malicious websites, modify the user interface, or exfiltrate data from the browser. However, session-related sensitive cookies are protected using the httpOnly flag, which mitigates the risk of session hijacking.	6.1	More Details
CVE-2025-57452	In realme BackupRestore app v15.1.12_2810c08_250314, improper URI scheme handling in com.coloros.pc.PcToolMainActivity allows local attackers to cause a crash and potential XSS via crafted ADB intents.	6.1	More Details
CVE-2025-56762	Paracrawl KeOPs v2 is vulnerable to Cross Site Scripting (XSS) in error.php.	6.1	More Details
CVE-2025-30755	OpenGrok 1.14.1 has a reflected Cross-Site Scripting (XSS) issue when producing the cross reference page. This happens through improper handling of the revision parameter. The application reflects unsanitized user input into the HTML output.	6.1	More Details
CVE-2025-53462	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SAPO SAPO Feed allows Stored XSS. This issue affects SAPO Feed: from n/a through 2.4.2.	5.9	More Details
CVE-2025-57929	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kanwei_doublethedonation Double the Donation allows Stored XSS. This issue affects Double the Donation: from n/a through 2.0.0.	5.9	More Details
CVE-2025-57974	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tuyennv TZ PlusGallery allows Stored XSS. This issue affects TZ PlusGallery: from n/a through 1.5.5.	5.9	More Details
CVE-2025-58245	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bestweblayout Portfolio allows DOM-Based XSS. This issue affects Portfolio : from n/a through 2.58.	5.9	More Details
CVE-2025-58223	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Taylor VoucherPress allows Stored XSS. This issue affects VoucherPress: from n/a through 1.5.7.	5.9	More Details
CVE-2025-58271	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AnyClip Video Platform AnyClip Luminous Studio allows Stored XSS. This issue affects AnyClip Luminous Studio: from n/a through 1.3.3.	5.9	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly	5.9	More

53467	Login-Logout allows Stored XSS. This issue affects Login-Logout: from n/a through 3.8.		Details
CVE-2025-53466	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeSolz Better Find and Replace allows Stored XSS. This issue affects Better Find and Replace: from n/a through 1.7.6.	5.9	More Details
CVE-2025-36064	IBM Sterling Connect:Express for Microsoft Windows 3.1.0.0 through 3.1.0.22 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.	5.9	More Details
CVE-2025-57882	An improper resource shutdown or release vulnerability has been identified in the Click Plus C2-03CPU-2 device running firmware version 3.60. The vulnerability allows an unauthenticated attacker to perform a denial-of-service attack by exhausting all available device sessions in the Remote PLC application.	5.9	More Details
CVE-2025-53469	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mortgage Calculator BMI Adult & Kid Calculator allows Stored XSS. This issue affects BMI Adult & Kid Calculator: from n/a through 1.2.2.	5.9	More Details
CVE-2025-58646	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chtombleson Mobi2Go allows Stored XSS. This issue affects Mobi2Go: from n/a through 1.0.0.	5.9	More Details
CVE-2025-57998	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hamid Reza Yazdani E-namad & Shamed Logo Manager allows Stored XSS. This issue affects E-namad & Shamed Logo Manager: from n/a through 2.2.	5.9	More Details
CVE-2025-53464	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ironikus WP Mailto Links allows Stored XSS. This issue affects WP Mailto Links: from n/a through 3.1.4.	5.9	More Details
CVE-2025-53455	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CashBill CashBill.pl – Płatności WooCommerce allows Stored XSS. This issue affects CashBill.pl – Płatności WooCommerce: from n/a through 3.2.1.	5.9	More Details
CVE-2025-57952	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in icopydoc Maps for WP allows Stored XSS. This issue affects Maps for WP: from n/a through 1.2.5.	5.9	More Details
CVE-2025-58645	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gravitate Gravitate Automated Tester allows Stored XSS. This issue affects Gravitate Automated Tester: from n/a through 1.4.5.	5.9	More Details
CVE-2025-53458	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in davaxi Goracash allows Stored XSS. This issue affects Goracash: from n/a through 1.1.	5.9	More Details
CVE-2025-53459	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ads by WPQuads Ads by WPQuads allows Stored XSS. This issue affects Ads by WPQuads: from n/a through 2.0.92.	5.9	More Details
CVE-2025-53460	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi AffiliateWP – External Referral Links allows Stored XSS. This issue affects AffiliateWP – External Referral Links: from n/a through 1.2.0.	5.9	More Details
CVE-2025-58674	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WordPress allows Stored XSS. WordPress core security team is aware of the issue and working on a fix. This is low severity vulnerability that requires an attacker to have Author or higher user privileges to execute the attack vector. This issue affects WordPress: from n/a through 6.8.2.	5.9	More Details
CVE-2025-57912	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dialogity Dialogity Free Live Chat allows Stored XSS. This issue affects Dialogity Free Live Chat: from n/a through 1.0.3.	5.9	More Details
CVE-2025-58655	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mattia Roccoberton Category Featured Images allows Stored XSS. This issue affects Category Featured Images: from n/a through 1.1.8.	5.9	More Details
CVE-2025-58033	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in leeshadle Draft allows Stored XSS. This issue affects Draft: from n/a through 3.0.9.	5.9	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant allows Stored XSS. This issue affects Media Library Assistant: from n/a	5.9	More Details

59590	through 3.28.		
CVE-2025-57956	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpcraft WooMS allows Stored XSS. This issue affects WooMS: from n/a through 9.12.	5.9	More Details
CVE-2025-57959	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tmatsuur Slightly troublesome permalink allows Stored XSS. This issue affects Slightly troublesome permalink: from n/a through 1.2.0.	5.9	More Details
CVE-2025-57979	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson AuthorSure allows Stored XSS. This issue affects AuthorSure: from n/a through 2.3.	5.9	More Details
CVE-2025-58960	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brijeshk89 IP Based Login allows Stored XSS. This issue affects IP Based Login: from n/a through 2.4.3.	5.9	More Details
CVE-2025-57980	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomas Cordero Safety Exit allows Stored XSS. This issue affects Safety Exit: from n/a through 1.8.0.	5.9	More Details
CVE-2025-57908	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ProWCPlugins Product Time Countdown for WooCommerce allows Stored XSS. This issue affects Product Time Countdown for WooCommerce: from n/a through 1.6.4.	5.9	More Details
CVE-2025-57906	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in epeken Epeken All Kurir allows Stored XSS. This issue affects Epeken All Kurir: from n/a through 2.0.2.	5.9	More Details
CVE-2025-57904	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP-EXPERTS.IN Sales Count Manager for WooCommerce allows Stored XSS. This issue affects Sales Count Manager for WooCommerce: from n/a through 2.5.	5.9	More Details
CVE-2025-57903	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPSuperiors Developer WooCommerce Additional Fees On Checkout (Free) allows Stored XSS. This issue affects WooCommerce Additional Fees On Checkout (Free): from n/a through 1.5.0.	5.9	More Details
CVE-2025-57982	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean Advance Portfolio Grid allows Stored XSS. This issue affects Advance Portfolio Grid: from n/a through 1.07.6.	5.9	More Details
CVE-2025-57945	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cedcommerce WP Advanced PDF allows Stored XSS. This issue affects WP Advanced PDF: from n/a through 1.1.7.	5.9	More Details
CVE-2025-57941	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JonathanMH Append Link on Copy allows Stored XSS. This issue affects Append Link on Copy: from n/a through 0.2.	5.9	More Details
CVE-2025-57951	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ken107 SiteNarrator Text-to-Speech Widget allows Stored XSS. This issue affects SiteNarrator Text-to-Speech Widget: from n/a through 1.9.	5.9	More Details
CVE-2025-57940	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Suresh Kumar Mukhiya Append extensions on Pages allows Stored XSS. This issue affects Append extensions on Pages: from n/a through 1.1.2.	5.9	More Details
CVE-2025-58669	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Modern Minds Magento 2 WordPress Integration allows Stored XSS. This issue affects Magento 2 WordPress Integration: from n/a through 1.4.1.	5.9	More Details
CVE-2025-57950	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Glen Scott Plugin Security Scanner allows Stored XSS. This issue affects Plugin Security Scanner: from n/a through 2.0.2.	5.9	More Details
CVE-2025-57920	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CK MacLeod Category Featured Images Extended allows Stored XSS. This issue affects Category Featured Images Extended: from n/a through 1.52.	5.9	More Details
CVE-2025-58256	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Brinley DOAJ Export allows Stored XSS. This issue affects DOAJ Export: from n/a through 1.0.4.	5.9	More Details

CVE-2025-57935	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ricky Dawn Bot Block – Stop Spam Referrals in Google Analytics allows Stored XSS. This issue affects Bot Block – Stop Spam Referrals in Google Analytics: from n/a through 2.6.	5.9	More Details
CVE-2025-58665	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tmontg1 Form Generator for WordPress allows Stored XSS. This issue affects Form Generator for WordPress: from n/a through 1.5.2.	5.9	More Details
CVE-2025-58266	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fumiki Takahashi Gianism allows Stored XSS. This issue affects Gianism: from n/a through 5.2.2.	5.9	More Details
CVE-2025-58661	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eZee Technosys eZee Online Hotel Booking Engine allows Stored XSS. This issue affects eZee Online Hotel Booking Engine: from n/a through 1.0.0.	5.9	More Details
CVE-2025-58658	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proof Factor LLC Proof Factor – Social Proof Notifications allows Stored XSS. This issue affects Proof Factor – Social Proof Notifications: from n/a through 1.0.5.	5.9	More Details
CVE-2025-57962	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Stored XSS. This issue affects VikRestaurants Table Reservations and Take-Away: from n/a through 1.4.	5.9	More Details
CVE-2025-58647	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Will.I.am Simple Restaurant Menu allows Stored XSS. This issue affects Simple Restaurant Menu: from n/a through 1.2.	5.9	More Details
CVE-2025-58473	An improper resource shutdown or release vulnerability has been identified in the Click Plus C2-03CPU-2 device running firmware version 3.60. The vulnerability allows an unauthenticated attacker to perform a denial-of-service attack by exhausting all available device sessions of the Click Programming Software.	5.9	More Details
CVE-2025-10042	The Quiz Maker plugin for WordPress is vulnerable to SQL Injection via spoofed IP headers in all versions up to, and including, 6.7.0.56 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 in configurations where the server is set up to retrieve the IP from a user-supplied field like `X-Forwarded-For` and limit users by IP is enabled.	5.9	More Details
CVE-2025-59797	Profession Fit 5.0.99 Build 44910 allows authorization bypass via a direct request for /api/challenges/{id} and also URLs for eversports, the user-management page, and the plane page.	5.8	More Details
CVE-2025-9115	The Etsy Shop WordPress plugin before 3.0.7 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers.	5.6	More Details
CVE-2025-36139	IBM Lakehouse (watsonx.data 2.2) is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.5	More Details
CVE-2025-59567	Missing Authorization vulnerability in Elliot Sowersby / RelyWP Coupon Affiliates allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Coupon Affiliates: from n/a through 6.8.0.	5.5	More Details
CVE-2025-59456	In JetBrains TeamCity before 2025.07.2 path traversal was possible during project archive upload	5.5	More Details
CVE-2025-46711	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger NULL pointer dereference kernel exceptions.	5.5	More Details
CVE-2025-57973	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chad Butler WP-Members allows Stored XSS. This issue affects WP-Members: from n/a through 3.5.4.2.	5.5	More Details
CVE-2025-59562	Authorization Bypass Through User-Controlled Key vulnerability in Academy LMS Academy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Academy LMS: from n/a through 3.3.4.	5.5	More Details
CVE-2025-59418	BunnyPad is a note taking software. Prior to version 11.0.27000.0915, opening files greater than or equal to 20MB causes buffer overflow to occur. This issue has been patched in version 11.0.27000.0915. Users who wish not to upgrade should refrain from opening files larger than 10MB.	5.5	More Details

CVE-2025-52367	Cross Site Scripting vulnerability in PivotX CMS v.3.0.0 RC 3 allows a remote attacker to execute arbitrary code via the subtitle field.	5.4	More Details
CVE-2025-58667	Missing Authorization vulnerability in CridioStudio ListingPro Reviews allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ListingPro Reviews: from n/a through 1.6.	5.4	More Details
CVE-2025-58660	Missing Authorization vulnerability in brandexponents Oshine Core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Oshine Core: from n/a through 1.5.5.	5.4	More Details
CVE-2025-57990	Missing Authorization vulnerability in solwininfotech Blog Designer allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Blog Designer: from n/a through 3.1.8.	5.4	More Details
CVE-2025-57991	Missing Authorization vulnerability in Clariti Clariti allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Clariti: from n/a through 1.2.1.	5.4	More Details
CVE-2025-58650	Missing Authorization vulnerability in Syed Balkhi All In One SEO Pack allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects All In One SEO Pack: from n/a through 4.8.7.	5.4	More Details
CVE-2025-59717	In the @digitalocean/do-markdownit package through 1.16.1 (in npm), the callout and fence_environment plugins perform .includes substring matching if allowedClasses or allowedEnvironments is a string (instead of an array).	5.4	More Details
CVE-2025-36037	IBM webMethods Integration 10.15 and 11.1 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2025-8487	The Kubio AI Page Builder plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the kubio-image-hub-install-plugin AJAX action in all versions up to, and including, 2.6.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install the Image Hub plugin.	5.4	More Details
CVE-2025-57946	Cross-Site Request Forgery (CSRF) vulnerability in Loc Bui payOS allows Cross Site Request Forgery. This issue affects payOS: from n/a through 1.0.61.	5.4	More Details
CVE-2025-58672	Missing Authorization vulnerability in Tareq Hasan WP User Frontend allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP User Frontend: from n/a through 4.1.11.	5.4	More Details
CVE-2025-57949	Missing Authorization vulnerability in oggix Ongkoskirim.id allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ongkoskirim.id: from n/a through 1.0.6.	5.4	More Details
CVE-2025-58673	Improper Control of Generation of Code ('Code Injection') vulnerability in Tareq Hasan WP User Frontend allows Code Injection. This issue affects WP User Frontend: from n/a through 4.1.11.	5.4	More Details
CVE-2025-35431	CISA Thorium does not escape user controlled strings used in LDAP queries. An authenticated remote attacker can modify LDAP authorization data such as group memberships. Fixed in 1.1.1.	5.4	More Details
CVE-2025-57880	Improper Encoding or Escaping of Output vulnerability in Hallo Welt! GmbH BlueSpice (Extension:BlueSpiceWhoIsOnline) allows Cross-Site Scripting (XSS). This issue affects BlueSpice: from 5 through 5.1.1.	5.4	More Details
CVE-2025-53451	Cross-Site Request Forgery (CSRF) vulnerability in mihdan Mihdan: No External Links allows Cross Site Request Forgery. This issue affects Mihdan: No External Links: from n/a through 5.1.4.	5.4	More Details
CVE-2025-26517	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a privilege escalation vulnerability. Successful exploit could allow an unauthorized authenticated attacker to discover Grid node names and IP addresses or modify Storage Grades.	5.4	More Details
CVE-2025-57994	Authorization Bypass Through User-Controlled Key vulnerability in Sayful Islam Upcoming Events Lists allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Upcoming Events Lists: from n/a through 1.4.0.	5.4	More Details

CVE-2025-59412	CubeCart is an ecommerce software solution. Prior to version 6.5.11, a vulnerability exists in the product reviews feature where user-supplied input is not properly sanitized before being displayed. An attacker can submit HTML tags inside the review description field. Once the administrator approves the review, the injected HTML is rendered on the product page for all visitors. This could be used to redirect users to malicious websites or to display unwanted content. This issue has been patched in version 6.5.11.	5.4	More Details
CVE-2025-10188	The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.4. This is due to missing or incorrect nonce validation on the bulk_remove() function. This makes it possible for unauthenticated attackers to arbitrary directory deletion in /wp-content via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2025-58224	Cross-Site Request Forgery (CSRF) vulnerability in Printeers Printeers Print & Ship allows Cross Site Request Forgery. This issue affects Printeers Print & Ship: from n/a through 1.17.0.	5.4	More Details
CVE-2025-56075	A SQL Injection vulnerability was discovered in the normal-bwdates-reports-details.php file of PHPGurukul Park Ticketing Management System v2.0. This vulnerability allows remote attackers to execute arbitrary SQL code via the fromdate parameter in a POST request.	5.4	More Details
CVE-2025-36248	IBM Copy Services Manager 6.3.13 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2025-9035	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Horato Internet Technologies Ind. And Trade Inc. Virtual Library Platform allows Reflected XSS.This issue affects Virtual Library Platform: before v202.	5.4	More Details
CVE-2025-59411	CubeCart is an ecommerce software solution. Prior to version 6.5.11, the contact form’s Enquiry field accepts raw HTML and that HTML is included verbatim in the email sent to the store admin. By submitting HTML in the Enquiry, the admin receives an email containing that HTML. This indicates user input is not being escaped or sanitized before being output in email (and possibly when re-rendering the form), leading to Cross-Site Scripting / HTML injection risk in email clients or admin UI. This issue has been patched in version 6.5.11.	5.4	More Details
CVE-2025-58005	Server-Side Request Forgery (SSRF) vulnerability in SmartDataSoft DriCub allows Server Side Request Forgery. This issue affects DriCub: from n/a through 2.9.	5.4	More Details
CVE-2025-59351	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the first return value of a function is dereferenced even when the function returns an error. This can result in a nil dereference, and cause code to panic. This vulnerability is fixed in 2.1.0.	5.3	More Details
CVE-2025-58659	Use of Hard-coded Credentials vulnerability in Essekia Helpie FAQ allows Retrieve Embedded Sensitive Data. This issue affects Helpie FAQ: from n/a through 1.39.	5.3	More Details
CVE-2025-58679	Missing Authorization vulnerability in AppMySite AppMySite allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AppMySite: from n/a through 3.14.0.	5.3	More Details
CVE-2025-10716	A flaw has been found in Creality Cloud App up to 6.1.0 on Android. Affected by this vulnerability is an unknown functionality of the file AndroidManifest.xml of the component com.cxsw.sdprinter. Executing manipulation can lead to improper export of android application components. It is possible to launch the attack on the local host. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-10305	The Secure Passkeys plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the delete_passkey() and passkeys_list() function in all versions up to, and including, 1.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view and delete passkeys.	5.3	More Details
CVE-2025-57971	Missing Authorization vulnerability in SALESmanago SALESmanago allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SALESmanago: from n/a through 3.8.1.	5.3	More Details
CVE-2025-58029	Missing Authorization vulnerability in Sumit Singh Classic Widgets with Block-based Widgets allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Classic Widgets with Block-based Widgets: from n/a through 1.0.1.	5.3	More Details
CVE-2025-58222	Missing Authorization vulnerability in Maidul Team Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Team Manager: from n/a through 2.3.14.	5.3	More Details

CVE-2025-58656	Use of Hard-coded Credentials vulnerability in Risto Niinemets Estonian Shipping Methods for WooCommerce allows Retrieve Embedded Sensitive Data. This issue affects Estonian Shipping Methods for WooCommerce: from n/a through 1.7.2.	5.3	More Details
CVE-2025-58000	Missing Authorization vulnerability in memberful Memberful allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Memberful: from n/a through 1.75.0.	5.3	More Details
CVE-2025-10709	A vulnerability was detected in Four-Faith Water Conservancy Informatization Platform 1.0. Affected by this issue is some unknown functionality of the file /history/historyDownload.do;otheruserLogin.do;getfile. The manipulation of the argument fileName results in path traversal. The attack can be executed 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.	5.3	More Details
CVE-2025-10708	A security vulnerability has been detected in Four-Faith Water Conservancy Informatization Platform 1.0. Affected by this vulnerability is an unknown functionality of the file /history/historyDownload.do;usrlogout.do. The manipulation of the argument fileName leads to path traversal. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-58226	Insertion of Sensitive Information Into Sent Data vulnerability in iberezansky 3D FlipBook – PDF Flipbook Viewer, Flipbook Image Gallery allows Retrieve Embedded Sensitive Data. This issue affects 3D FlipBook – PDF Flipbook Viewer, Flipbook Image Gallery: from n/a through 1.16.16.	5.3	More Details
CVE-2025-58003	Missing Authorization vulnerability in javothemes Javo Core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Javo Core: from n/a through 3.0.0.266.	5.3	More Details
CVE-2025-10759	A vulnerability was detected in Webkul QloApps up to 1.7.0. This affects an unknown function of the component CSRF Token Handler. Performing manipulation of the argument token results in authorization bypass. The attack may be initiated remotely. The exploit is now public and may be used. The vendor explains: "As We are already aware about this vulnerability and our Internal team are already working on this issue. (...) We'll implement the fix for this vulnerability in our next major release."	5.3	More Details
CVE-2024-25011	Ericsson Catalog Manager and Ericsson Order Care APIs do not have authentication enabled by default. Authentication checks can be configured to remediate the information disclosure issue.	5.3	More Details
CVE-2025-58015	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Ays Pro Quiz Maker allows Retrieve Embedded Sensitive Data. This issue affects Quiz Maker: from n/a through 6.7.0.61.	5.3	More Details
CVE-2025-10493	The Chained Quiz plugin for WordPress is vulnerable to Insecure Direct Object Reference in version 1.3.4 and below via the quiz submission and completion mechanisms due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to hijack and modify other users' quiz attempts by manipulating the chained_completion_id cookie value, allowing them to alter quiz answers, scores, and results of any user. The vulnerability was partially patched in versions 1.3.4 and 1.3.5.	5.3	More Details
CVE-2025-58247	Missing Authorization vulnerability in templateinvaders TI WooCommerce Wishlist allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects TI WooCommerce Wishlist: from n/a through 2.10.0.	5.3	More Details
CVE-2025-58685	Missing Authorization vulnerability in cecabank Cecabank WooCommerce Plugin allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Cecabank WooCommerce Plugin: from n/a through 0.3.4.	5.3	More Details
CVE-2025-57987	Missing Authorization vulnerability in ThimPress WP Events Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Events Manager: from n/a through 2.2.1.	5.3	More Details
CVE-2025-58004	Missing Authorization vulnerability in SmartDataSoft DriCub allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects DriCub: from n/a through 2.9.	5.3	More Details
CVE-2025-57976	Missing Authorization vulnerability in CardCom CardCom Payment Gateway allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CardCom Payment Gateway: from n/a through 3.5.0.4.	5.3	More Details
CVE-2025-59354	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the DragonFly2 uses a variety of hash functions, including the MD5 hash, for downloaded files. This allows attackers to replace files with malicious ones that have a colliding hash. This vulnerability is fixed in 2.1.0.	5.3	More Details
	Dragonfly is an open source P2P-based file distribution and image acceleration system. Versions prior to 2.1.0		

CVE-2025-59346	contain a server-side request forgery (SSRF) vulnerability that enables users to force DragonFly2's components to make requests to internal services that are otherwise not accessible to them. The issue arises because the Manager API accepts a user-supplied URL when creating a Preheat job with weak validation, peers can trigger other peers to fetch an arbitrary URL through pieceManager.DownloadSource, and internal HTTP clients follow redirects, allowing a request to a malicious server to be redirected to internal services. This can be used to probe or access internal HTTP endpoints. The vulnerability is fixed in version 2.1.0.	5.3	More Details
CVE-2025-59350	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the access control mechanism for the Proxy feature uses simple string comparisons and is therefore vulnerable to timing attacks. An attacker may try to guess the password one character at a time by sending all possible characters to a vulnerable mechanism and measuring the comparison instruction's execution times. This vulnerability is fixed in 2.1.0.	5.3	More Details
CVE-2025-58269	Use of Hard-coded Credentials vulnerability in weDevs WP Project Manager allows Retrieve Embedded Sensitive Data. This issue affects WP Project Manager: from n/a through 2.6.25.	5.3	More Details
CVE-2025-58681	Missing Authorization vulnerability in Jürgen Müller Easy Quotes allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Easy Quotes: from n/a through 1.2.4.	5.3	More Details
CVE-2025-10715	A security flaw has been discovered in APEUni PTE Exam Practice App up to 10.8.0 on Android. The impacted element is an unknown function of the file AndroidManifest.xml of the component com.ape_edication. The manipulation results in improper export of android application components. The attack requires a local approach. 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.	5.3	More Details
CVE-2025-10717	A vulnerability has been found in intsig CamScanner App 6.91.1.5.250711 on Android. Affected by this issue is some unknown functionality of the file AndroidManifest.xml of the component com.intsig.camscanner. The manipulation leads to improper export of android application components. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-57928	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Strategy11 Team AWP Classifieds allows Code Injection. This issue affects AWP Classifieds: from n/a through 4.3.5.	5.3	More Details
CVE-2025-59573	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in CozyThemes Cozy Blocks allows Code Injection. This issue affects Cozy Blocks: from n/a through 2.1.29.	5.3	More Details
CVE-2025-59582	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Darren Cooney Ajax Load More allows Retrieve Embedded Sensitive Data. This issue affects Ajax Load More: from n/a through 7.6.0.2.	5.3	More Details
CVE-2025-57939	Missing Authorization vulnerability in Blocksera Image Hover Effects – Elementor Addon allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Image Hover Effects – Elementor Addon: from n/a through 1.4.4.	5.3	More Details
CVE-2025-59433	Conventional Changelog generates changelogs and release notes from a project's commit messages and metadata. Prior to version 2.0.0, @conventional-changelog/git-client has an argument injection vulnerability. This vulnerability manifests with the library's getTags() API, which allows extra parameters to be passed to the git log command. In another API by this library, getRawCommits(), there are secure practices taken to ensure that the extra parameter path is unable to inject an argument by ending the git log command with the special shell syntax --. However, the library does not follow the same practice for getTags() as it does not attempt to sanitize for user input, validate the given params, or restrict them to an allow list. Nor does it properly pass command-line flags to the git binary using the double-dash POSIX characters (--) to communicate the end of options. Thus, allowing users to exploit an argument injection vulnerability in Git due to the --output= command-line option that results with overwriting arbitrary files. This issue has been patched in version 2.0.0.	5.3	More Details
CVE-2025-59547	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, the CKEditor file upload endpoint has insufficient sanitization for filenames allowing probing network endpoints. A specially crafted request can be made to upload a file with Unicode characters, which would be translated into a path that could expose resources in the internal network of the hosted site. This issue has been patched in version 10.1.0.	5.3	More Details
CVE-2025-57899	Missing Authorization vulnerability in AresIT WP Compress allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WP Compress: from n/a through 6.50.54.	5.3	More Details
CVE-2025-	A vulnerability was determined in axboe fio up to 3.41. This impacts the function __parse_jobs_ini of the file init.c. Executing manipulation can lead to use after free. The attack needs to be launched locally. The exploit	5.3	More

10824	has been publicly disclosed and may be utilized.		Details
CVE-2025-57922	Insertion of Sensitive Information Into Sent Data vulnerability in Coordinadora Mercantil S.A. Envíos Coordinadora Woocommerce allows Retrieve Embedded Sensitive Data. This issue affects Envíos Coordinadora Woocommerce: from n/a through 1.1.31.	5.3	More Details
CVE-2025-57923	Insertion of Sensitive Information Into Sent Data vulnerability in Ideal Postcodes UK Address Postcode Validation allows Retrieve Embedded Sensitive Data. This issue affects UK Address Postcode Validation: from n/a through 3.9.2.	5.3	More Details
CVE-2025-58969	Missing Authorization vulnerability in Greg Winiarski Custom Login URL allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Custom Login URL: from n/a through 1.0.2.	5.3	More Details
CVE-2025-26516	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a Denial of Service vulnerability. Successful exploit could allow an unauthenticated attacker to cause a Denial of Service on the Admin node.	5.3	More Details
CVE-2025-8463	Authorization Bypass Through User-Controlled Key vulnerability in SecHard Information Technologies SecHard allows Parameter Injection.This issue affects SecHard: before 3.6.2-20250805.	5.3	More Details
CVE-2025-54467	When a Java command with password parameters is executed and terminated by NeuVector for Process rule violation the password will appear in the NeuVector security event log.	5.3	More Details
CVE-2025-53884	NeuVector stores user passwords and API keys using a simple, unsalted hash. This method is vulnerable to rainbow table attack (offline attack where hashes of known passwords are precomputed).	5.3	More Details
CVE-2025-10722	A vulnerability was detected in SKTLab Mukbee App 1.01.196 on Android. This affects an unknown function of the file AndroidManifest.xml of the component com.dw.android.mukbee. The manipulation results in improper export of android application components. The attack must be initiated from a local position. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-10721	A vulnerability was determined in Webull Investing & Trading App 11.2.5.63 on Android. This vulnerability affects unknown code of the file AndroidManifest.xml. This manipulation causes improper export of android application components. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-8999	The Sydney theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'activate_modules' function in all versions up to, and including, 2.56. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate or deactivate various theme modules.	5.3	More Details
CVE-2025-56869	Directory traversal vulnerability in Sync In server thru 1.1.1 allowing authenticated attackers to gain read and write access to the system via FilesManager.saveMultipart function in backend/src/applications/files/services/files-manager.service.ts, and FilesManager.compress function in backend/src/applications/files/services/files-manager.service.ts.	5.3	More Details
CVE-2025-57944	Missing Authorization vulnerability in Skimlinks Skimlinks Affiliate Marketing Tool allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Skimlinks Affiliate Marketing Tool: from n/a through 1.3.	5.3	More Details
CVE-2025-57907	Missing Authorization vulnerability in Heureka Group Heureka allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Heureka: from n/a through 1.1.0.	5.3	More Details
CVE-2025-58069	The use of a hard-coded cryptographic key was discovered in firmware version 3.60 of the Click Plus PLC. The vulnerability relies on the fact that the software contains a hard-coded AES key used to protect the initial messages of a new KOPS session.	5.3	More Details
CVE-2025-35436	CISA Thorium uses '.unwrap()' to handle errors related to account verification email messages. An unauthenticated remote attacker could cause a crash by providing a specially crafted email address or response. Fixed in commit 6a65a27.	5.3	More Details
CVE-2025-57958	Missing Authorization vulnerability in WPXPO WowAddons allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WowAddons: from n/a through 1.0.17.	5.3	More Details
CVE-	A vulnerability was found in Ooma Office Business Phone App up to 7.2.2 on Android. This affects an unknown part of the component com.ooma.office2. The manipulation results in improper export of android application		More

2025-10718	components. The attack needs to be approached locally. 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	Details
CVE-2025-57957	Missing Authorization vulnerability in wpcraft WooMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WooMS: from n/a through 9.12.	5.3	More Details
CVE-2025-35432	CISA Thorium does not rate limit requests to send account verification email messages. A remote unauthenticated attacker can send unlimited messages to a user who is pending verification. Fixed in 1.1.1 by adding a rate limit set by default to 10 minutes.	5.3	More Details
CVE-2025-57921	Missing Authorization vulnerability in N-Media Frontend File Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Frontend File Manager: from n/a through 23.2.	5.3	More Details
CVE-2025-25177	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger use-after-free kernel exceptions.	5.1	More Details
CVE-2024-21935	Improper input validation in Satellite Management Controller (SMC) may allow an attacker with privileges to manipulate Redfish® API commands to remove files from the local root directory, potentially resulting in data corruption.	5.0	More Details
CVE-2025-58968	Missing Authorization vulnerability in Christiaan Pieterse MaxiBlocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MaxiBlocks: from n/a through 2.1.3.	5.0	More Details
CVE-2025-35433	CISA Thorium does not properly invalidate previously used tokens when resetting passwords. An attacker that possesses a previously used token could still log in after a password reset. Fixed in 1.1.1.	5.0	More Details
CVE-2025-35430	CISA Thorium does not adequately validate the paths of downloaded files via 'download_ephemeral' and 'download_children'. A remote, authenticated attacker could access arbitrary files subject to file system permissions. Fixed in 1.1.2.	5.0	More Details
CVE-2024-21927	Improper input validation in Satellite Management Controller (SMC) may allow an attacker with privileges to use certain special characters in manipulated Redfish® API commands, causing service processes like OpenBMC to crash and reset, potentially resulting in denial of service.	5.0	More Details
CVE-2025-55075	Hidden functionality issue exists in WN-7D36QR and WN-7D36QR/UE. If this vulnerability is exploited, SSH may be enabled by a remote authenticated attacker.	4.9	More Details
CVE-2025-10002	The ClickWhale – Link Manager, Link Shortener and Click Tracker for Affiliate Links & Link Pages plugin for WordPress is vulnerable to SQL Injection via the export_csv() function in all versions up to, and including, 2.5.0 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 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. This may be exploitable by lower level users if access to the plugin is granted.	4.9	More Details
CVE-2025-59715	SMSEagle before 6.11 allows reflected XSS via a username or contact phone number.	4.8	More Details
CVE-2025-58114	Improper Input Validation vulnerability in Hallo Welt! GmbH BlueSpice (Extension:CognitiveProcessDesigner) allows Cross-Site Scripting (XSS).This issue affects BlueSpice: from 5 through 5.1.1.	4.8	More Details
CVE-2025-4760	An authenticated stored cross-site scripting (XSS) vulnerability exists in multiple WSO2 products due to improper validation of user-supplied input during API document upload in the Publisher portal. A user with publisher privileges can upload a crafted API document containing malicious JavaScript, which is later rendered in the browser when accessed by other users. A successful attack could result in redirection to malicious websites, unauthorized UI modifications, or exfiltration of browser-accessible data. However, session-related sensitive cookies are protected by the httpOnly flag, preventing session hijacking.	4.8	More Details
CVE-2025-0546	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting'), Improper Restriction of Rendered UI Layers or Frames vulnerability in Mevzuattr Software MevzuatTR allows Phishing, iFrame Overlay, Clickjacking, Forceful Browsing. This issue needs high privileges. This issue affects MevzuatTR: before 12.02.2025.	4.7	More Details
CVE-2025-36143	IBM Lakehouse (watsonx.data 2.2) could allow an authenticated privileged user to execute arbitrary commands on the system due to improper validation of user supplied input.	4.7	More Details

CVE-2025-7702	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Pusula Communication Information Internet Industry and Trade Ltd. Co. Manageable Email Sending System allows Exploiting Trust in Client.This issue affects Manageable Email Sending System: from <=2025.06 before 2025.08.06.	4.7	More Details
CVE-2025-58006	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks WP Gravity Forms Keap/Infusionsoft allows Phishing. This issue affects WP Gravity Forms Keap/Infusionsoft: from n/a through 1.2.4.	4.7	More Details
CVE-2025-9540	The Markup Markdown WordPress plugin before 3.20.10 allows links to contain JavaScript which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	4.7	More Details
CVE-2025-10662	A vulnerability has been found in SeaCMS up to 13.3. The impacted element is an unknown function of the file /admin_members.php?ac=editsave. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This affects another injection point than CVE-2025-25513.	4.7	More Details
CVE-2025-10774	A weakness has been identified in Ruijie 6000-E10 up to 2.4.3.6-20171117. This affects an unknown part of the file /view/vpn/autovpn/sub_commit.php. This manipulation of the argument key causes os command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-9541	The Markup Markdown WordPress plugin before 3.20.10 allows links to contain JavaScript which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	4.7	More Details
CVE-2025-10765	A security flaw has been discovered in SeriaWei ZKEACMS up to 4.3. This vulnerability affects the function CheckPage/Suggestions in the library cms-v4.3\wwwroot\Plugins\ZKEACMS.SEOSuggestions\ZKEACMS.SEOSuggestions.dll of the component SEOSuggestions. Performing manipulation results in server-side request forgery. It is possible to initiate the attack 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.	4.7	More Details
CVE-2025-9487	The Admin and Site Enhancements (ASE) WordPress plugin before 7.9.8 does not sanitise SVG files when uploaded via xmlrpc.php when such uploads are enabled, which could allow users to upload a malicious SVG containing XSS payloads	4.7	More Details
CVE-2025-0420	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Paraşüt Software Paraşüt allows Cross-Site Scripting (XSS).This issue affects Paraşüt: from 0.0.0.65efa44e through 20250204.	4.7	More Details
CVE-2025-0547	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Paraşüt Software Bizmu allows Cross-Site Scripting (XSS).This issue affects Bizmu: from 2.27.0 through 20250212.	4.7	More Details
CVE-2025-0419	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zirve Information Technologies Inc. Zirve Nova allows Cross-Site Scripting (XSS).This issue affects Zirve Nova: from 235 through 20250131.	4.7	More Details
CVE-2025-10775	A security vulnerability has been detected in Wavlink WL-NU516U1 240425. This vulnerability affects the function sub_4012A0 of the file /cgi-bin/login.cgi. Such manipulation of the argument ipaddr leads to os command injection. It is possible to launch 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.	4.7	More Details
CVE-2025-0879	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Shopside Software Shopside App allows Cross-Site Scripting (XSS). This issue requires high privileges.This issue affects Shopside App: before 17.02.2025.	4.7	More Details
CVE-2025-8079	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akıllı Ticaret Software Technologies Ltd. Co. Smart Trade E-Commerce allows Reflected XSS.This issue affects Smart Trade E-Commerce: before 4.5.0.0.1.	4.6	More Details
CVE-2025-59415	Frappe Learning is a learning system that helps users structure their content. In versions 2.34.1 and below, there is a security vulnerability in Frappe Learning where the system did not adequately sanitize the content uploaded in the profile bio. Malicious SVG files could be used to execute arbitrary scripts in the context of other users.	4.6	More Details
CVE-2025-10767	A vulnerability was detected in CosmodiumCS OnlyRAT up to 3.2. The affected element is the function connect/remote_upload/remote_download of the file main.py of the component Configuration File Handler. The manipulation of the argument configuration["PASSWORD"] results in os command injection. The attack requires a local approach. Attacks of this nature are highly complex. The exploitability is described as difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but	4.5	More Details

	did not respond in any way.		
CVE-2025-53457	Server-Side Request Forgery (SSRF) vulnerability in activewebsight SEO Backlink Monitor allows Server Side Request Forgery. This issue affects SEO Backlink Monitor: from n/a through 1.6.0.	4.4	More Details
CVE-2025-59339	The Bastion provides authentication, authorization, traceability and auditability for SSH accesses. Session-recording ttyrec files, may be handled by the provided osh-encrypt-rsync script that is a helper to rotate, encrypt, sign, copy, and optionally move them to a remote storage periodically, if configured to. When running, the script properly rotates and encrypts the files using the provided GPG key(s), but silently fails to sign them, even if asked to.	4.4	More Details
CVE-2025-23336	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause a denial of service by loading a misconfigured model. A successful exploit of this vulnerability might lead to denial of service.	4.4	More Details
CVE-2025-53461	Server-Side Request Forgery (SSRF) vulnerability in Binsaifullah Beaf allows Server Side Request Forgery. This issue affects Beaf: from n/a through 1.6.2.	4.4	More Details
CVE-2025-57984	Server-Side Request Forgery (SSRF) vulnerability in Pratik Ghela MakeStories (for Google Web Stories) allows Server Side Request Forgery. This issue affects MakeStories (for Google Web Stories): from n/a through 3.0.4.	4.4	More Details
CVE-2025-57943	Server-Side Request Forgery (SSRF) vulnerability in Skimlinks Skimlinks Affiliate Marketing Tool allows Server Side Request Forgery. This issue affects Skimlinks Affiliate Marketing Tool: from n/a through 1.3.	4.4	More Details
CVE-2025-58016	Missing Authorization vulnerability in Codexpert, Inc CF7 Submissions allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CF7 Submissions: from n/a through 0.26.	4.3	More Details
CVE-2025-58007	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in NerdPress Social Pug allows Retrieve Embedded Sensitive Data. This issue affects Social Pug: from n/a through 1.35.1.	4.3	More Details
CVE-2025-58014	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Quiz Maker allows Cross Site Request Forgery. This issue affects Quiz Maker: from n/a through 6.7.0.61.	4.3	More Details
CVE-2025-57924	Cross-Site Request Forgery (CSRF) vulnerability in Automattic Developer allows Cross Site Request Forgery. This issue affects Developer: from n/a through 1.2.6.	4.3	More Details
CVE-2025-57917	Missing Authorization vulnerability in printcart Printcart Web to Print Product Designer for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Printcart Web to Print Product Designer for WooCommerce: from n/a through 2.4.3.	4.3	More Details
CVE-2025-58032	Cross-Site Request Forgery (CSRF) vulnerability in Bytes.co WP Compiler allows Cross Site Request Forgery. This issue affects WP Compiler: from n/a through 1.0.0.	4.3	More Details
CVE-2025-57916	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Nurul Amin WP System Information allows Retrieve Embedded Sensitive Data. This issue affects WP System Information: from n/a through 1.5.	4.3	More Details
CVE-2025-57930	Cross-Site Request Forgery (CSRF) vulnerability in kanwei_doublethedonation Double the Donation allows Cross Site Request Forgery. This issue affects Double the Donation: from n/a through 2.0.0.	4.3	More Details
CVE-2025-57927	Cross-Site Request Forgery (CSRF) vulnerability in Stephanie Leary Dashboard Notepad allows Cross Site Request Forgery. This issue affects Dashboard Notepad: from n/a through 1.42.	4.3	More Details
CVE-2025-57975	Missing Authorization vulnerability in RadiusTheme Team allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Team: from n/a through 5.0.6.	4.3	More Details
CVE-2025-57961	Missing Authorization vulnerability in Codexpert, Inc CoDesigner allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CoDesigner: from n/a through 4.25.2.	4.3	More Details
CVE-	Missing Authorization vulnerability in Jeremy Saxey Hide WP Toolbar allows Exploiting Incorrectly Configured		More

2025-57969	Access Control Security Levels. This issue affects Hide WP Toolbar: from n/a through 2.7.	4.3	Details
CVE-2025-57970	Cross-Site Request Forgery (CSRF) vulnerability in SALESmanago SALESmanago allows Cross Site Request Forgery. This issue affects SALESmanago: from n/a through 3.8.1.	4.3	More Details
CVE-2025-58199	Cross-Site Request Forgery (CSRF) vulnerability in Fastly Fastly allows Cross Site Request Forgery. This issue affects Fastly: from n/a through 1.2.28.	4.3	More Details
CVE-2025-53456	Cross-Site Request Forgery (CSRF) vulnerability in activewebsight SEO Backlink Monitor allows Cross Site Request Forgery. This issue affects SEO Backlink Monitor: from n/a through 1.6.0.	4.3	More Details
CVE-2025-57972	Missing Authorization vulnerability in WPFactory Helpdesk Support Ticket System for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Helpdesk Support Ticket System for WooCommerce: from n/a through 2.0.2.	4.3	More Details
CVE-2025-59040	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Backlog item representations do not verify the permissions of the child trackers. Users might see tracker names they should not have access to. This vulnerability is fixed in Tuleap Community Edition 16.11.99.1757427600 and Tuleap Enterprise Edition 16.11-6 and 16.10-8.	4.3	More Details
CVE-2025-53452	Missing Authorization vulnerability in Barry Event Rocket allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Event Rocket: from n/a through 3.3.	4.3	More Details
CVE-2025-57942	Cross-Site Request Forgery (CSRF) vulnerability in andy_moyle Emergency Password Reset allows Cross Site Request Forgery. This issue affects Emergency Password Reset: from n/a through 9.0.	4.3	More Details
CVE-2025-57937	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in etruel WPeMatico RSS Feed Fetcher allows Retrieve Embedded Sensitive Data. This issue affects WPeMatico RSS Feed Fetcher: from n/a through 2.8.10.	4.3	More Details
CVE-2025-57997	Missing Authorization vulnerability in Trustpilot Trustpilot Reviews allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Trustpilot Reviews: from n/a through 2.5.925.	4.3	More Details
CVE-2025-57978	Cross-Site Request Forgery (CSRF) vulnerability in themespride Advanced Appointment Booking & Scheduling allows Cross Site Request Forgery. This issue affects Advanced Appointment Booking & Scheduling: from n/a through 1.9.	4.3	More Details
CVE-2025-57985	Missing Authorization vulnerability in MantraBrain Ultimate Watermark allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ultimate Watermark: from n/a through 1.1.	4.3	More Details
CVE-2025-57936	Missing Authorization vulnerability in Meitar Subresource Integrity (SRI) Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Subresource Integrity (SRI) Manager: from n/a through 0.4.0.	4.3	More Details
CVE-2025-57934	Cross-Site Request Forgery (CSRF) vulnerability in Aurélien LWS LWS Affiliation allows Cross Site Request Forgery. This issue affects LWS Affiliation: from n/a through 2.3.6.	4.3	More Details
CVE-2025-57933	Cross-Site Request Forgery (CSRF) vulnerability in piotnetdotcom Piotnet Forms allows Cross Site Request Forgery. This issue affects Piotnet Forms: from n/a through 1.0.30.	4.3	More Details
CVE-2025-57960	Cross-Site Request Forgery (CSRF) vulnerability in TravelMap Travel Map allows Cross Site Request Forgery. This issue affects Travel Map: from n/a through 1.0.3.	4.3	More Details
CVE-2025-57905	Cross-Site Request Forgery (CSRF) vulnerability in Amin Y AgreeMe Checkboxes For WooCommerce allows Cross Site Request Forgery. This issue affects AgreeMe Checkboxes For WooCommerce: from n/a through 1.1.3.	4.3	More Details
CVE-2025-57992	Cross-Site Request Forgery (CSRF) vulnerability in InterServer Mail Baby SMTP allows Cross Site Request Forgery. This issue affects Mail Baby SMTP: from n/a through 2.8.	4.3	More Details
CVE-	Missing Authorization vulnerability in Detheme DethemeKit For Elementor allows Exploiting Incorrectly		More

2025-57995	Configured Access Control Security Levels. This issue affects DethemeKit For Elementor: from n/a through 2.1.10.	4.3	Details
CVE-2025-58010	Cross-Site Request Forgery (CSRF) vulnerability in straightvisions GmbH SV Proven Expert allows Cross Site Request Forgery. This issue affects SV Proven Expert: from n/a through 2.0.06.	4.3	More Details
CVE-2025-59799	Artifex Ghostscript through 10.05.1 has a stack-based buffer overflow in pdfmark_coerce_dest in devices/vector/gdevpdfm.c via a large size value.	4.3	More Details
CVE-2025-58200	Cross-Site Request Forgery (CSRF) vulnerability in Bage Flexible FAQ allows Cross Site Request Forgery. This issue affects Flexible FAQ: from n/a through 0.2.	4.3	More Details
CVE-2025-59568	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Flow Zoho Flow allows Cross Site Request Forgery. This issue affects Zoho Flow: from n/a through 2.14.1.	4.3	More Details
CVE-2025-58219	Cross-Site Request Forgery (CSRF) vulnerability in LIJE Show Pages List allows Cross Site Request Forgery. This issue affects Show Pages List: from n/a through 1.2.0.	4.3	More Details
CVE-2025-9887	The Custom Login And Signup Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation in the /frndzk_adminclsw.php file. This makes it possible for unauthenticated attackers to change the email and username 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-2025-9949	The Internal Links Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.1. This is due to missing or incorrect nonce validation on the link deletion functionality in the process_bulk_action() function. This makes it possible for unauthenticated attackers to delete SEO links 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-2025-10489	The SureForms – Drag and Drop Contact Form Builder – Multi-step Forms, Conversational Forms and more plugin for WordPress is vulnerable to unauthorized creation of forms due to a missing capability check on the register_post_types() function in all versions up to, and including, 1.12.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to create forms when the user interface specifically prohibits it.	4.3	More Details
CVE-2025-58675	Cross-Site Request Forgery (CSRF) vulnerability in tryinteract Interact: Embed A Quiz On Your Site allows Cross Site Request Forgery. This issue affects Interact: Embed A Quiz On Your Site: from n/a through 3.1.	4.3	More Details
CVE-2025-10607	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /module/Avaliacao/diarioApi. Such manipulation leads to information disclosure. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-10606	A weakness has been identified in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /module/Configuracao/ConfiguracaoMovimentoGeral. This manipulation of the argument tipoacao causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-10605	A security flaw has been discovered in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /agenda_preferencias.php. The manipulation of the argument tipoacao results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-35435	CISA Thorium accepts a stream split size of zero then divides by this value. A remote, authenticated attacker could cause the service to crash. Fixed in commit 89101a6.	4.3	More Details
CVE-2025-58957	Missing Authorization vulnerability in Vikas Ratudi VPSUForm allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects VPSUForm: from n/a through 3.2.20.	4.3	More Details
CVE-2025-59551	Missing Authorization vulnerability in WP Chill Revive.so allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Revive.so: from n/a through 2.0.6.	4.3	More Details
CVE-2025-	Missing Authorization vulnerability in payrexx Payrexx Payment Gateway for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Payrexx Payment Gateway for	4.3	More

59559	WooCommerce: from n/a through 3.1.5.		Details
CVE-2025-59561	Missing Authorization vulnerability in hashthemes Smart Blocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Smart Blocks: from n/a through 2.4.	4.3	More Details
CVE-2025-59577	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Stylemix MasterStudy LMS allows Leveraging Race Conditions. This issue affects MasterStudy LMS: from n/a through 3.6.20.	4.3	More Details
CVE-2025-10719	Tronclass developed by WisdomGarden has an Insecure Direct object Reference vulnerability, allowing remote attackers with regular privilege to modify a specific parameter to access other users' files.	4.3	More Details
CVE-2025-59591	Missing Authorization vulnerability in AdvancedCoding wpDiscuz allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpDiscuz: from n/a through 7.6.33.	4.3	More Details
CVE-2025-10819	A security vulnerability has been detected in fuyang_lipengjun platform 1.0. This issue affects the function UserCouponController of the file /usercoupon/queryAll. The manipulation leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-10820	A vulnerability was detected in fuyang_lipengjun platform 1.0. Impacted is the function TopicController of the file /topic/queryAll. The manipulation results in improper authorization. The attack can be executed remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2025-10821	A flaw has been found in fuyang_lipengjun platform 1.0. The affected element is the function TopicCategoryController of the file /topiccategory/queryAll. This manipulation causes improper authorization. The attack is possible to be carried out remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-10822	A vulnerability has been found in fuyang_lipengjun platform 1.0. The impacted element is the function SysSmsLogController of the file /sys/smslog/queryAll. Such manipulation leads to improper authorization. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-10827	A weakness has been identified in PHPJabbers Restaurant Menu Maker up to 1.1. Affected by this issue is some unknown functionality of the file /preview.php. This manipulation of the argument theme causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-42907	SAP BI Platform allows an attacker to modify the IP address of the LogonToken for the OpenDoc. On accessing the modified link in the browser a different server could get the ping request. This has low impact on integrity with no impact on confidentiality and availability of the system.	4.3	More Details
CVE-2025-50709	An issue in Perplexity AI GPT-4 allows a remote attacker to obtain sensitive information via a GET parameter	4.3	More Details
CVE-2025-10590	A security flaw has been discovered in Portabilis i-Educar up to 2.10. The impacted element is an unknown function of the file /intranet/educar_usuario_det.php. The manipulation of the argument ref_pessoa results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2024-6429	A content spoofing vulnerability exists in multiple WSO2 products due to improper error message handling. Under certain conditions, error messages are passed through URL parameters without validation, allowing malicious actors to inject arbitrary content into the UI. By exploiting this vulnerability, attackers can manipulate browser-displayed error messages, enabling social engineering attacks through deceptive or misleading content.	4.3	More Details
CVE-2025-58246	Insertion of Sensitive Information Into Sent Data vulnerability in Automattic WordPress allows Retrieve Embedded Sensitive Data. The WordPress Core security team is aware of the issue and is already working on a fix. This is a low-severity vulnerability. Contributor-level privileges required in order to exploit it. This issue affects WordPress: from n/a through 6.8.2	4.3	More Details
CVE-2025-9891	The User Sync – Remote User Sync 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 mo_user_sync_form_handler() function. This makes it possible for unauthenticated attackers to deactivate the plugin 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-	The USS Upyun plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.0. This is due to missing or incorrect nonce validation on the uss_setting_page function when processing the uss_set form type. This makes it possible for unauthenticated attackers to modify critical	4.3	More

9629	Upyun cloud storage settings including bucket name, operator credentials, upload paths, and image processing parameters via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		Details
CVE-2025-10710	A flaw has been found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 20250831. This affects an unknown part of the file /index.php. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10711	A vulnerability has been found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 20250831. This vulnerability affects unknown code of the file /index.php/sysmanage/Login. Such manipulation of the argument Name leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10630	Grafana is an open-source platform for monitoring and observability. Grafana-Zabbix is a plugin for Grafana allowing to visualize monitoring data from Zabbix and create dashboards for analyzing metrics and realtime monitoring. Versions 5.2.1 and below contained a ReDoS vulnerability via user-supplied regex query which could causes CPU usage to max out. This vulnerability is fixed in version 6.0.0.	4.3	More Details
CVE-2025-36146	IBM Lakehouse (watsonx.data 2.2) could allow an authenticated user to obtain sensitive server component version information which could aid in further attacks against the system.	4.3	More Details
CVE-2025-58221	Missing Authorization vulnerability in ONTRAPORT PilotPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PilotPress: from n/a through 2.0.35.	4.3	More Details
CVE-2025-58236	Cross-Site Request Forgery (CSRF) vulnerability in Mayo Moriyama Force Update Translations allows Cross Site Request Forgery. This issue affects Force Update Translations: from n/a through 0.5.	4.3	More Details
CVE-2025-58249	Insertion of Sensitive Information Into Sent Data vulnerability in Themeum Qubely allows Retrieve Embedded Sensitive Data. This issue affects Qubely: from n/a through 1.8.14.	4.3	More Details
CVE-2025-58251	Missing Authorization vulnerability in POSIMYTH Sticky Header Effects for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Sticky Header Effects for Elementor: from n/a through 2.1.2.	4.3	More Details
CVE-2025-10794	A flaw has been found in PHPGurukul Car Rental Project 3.0. Affected by this issue is some unknown functionality of the file /carrental/search.php. Executing manipulation of the argument autofocus can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-58252	Insertion of Sensitive Information Into Sent Data vulnerability in jetmonsters Getwid allows Retrieve Embedded Sensitive Data. This issue affects Getwid: from n/a through 2.1.2.	4.3	More Details
CVE-2025-58258	Missing Authorization vulnerability in nK Lazy Blocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Lazy Blocks: from n/a through 4.1.0.	4.3	More Details
CVE-2025-58649	Insertion of Sensitive Information Into Sent Data vulnerability in Syed Balkhi All In One SEO Pack allows Retrieve Embedded Sensitive Data. This issue affects All In One SEO Pack: from n/a through 4.8.7.	4.3	More Details
CVE-2025-10674	A vulnerability was identified in fuyang_lipengjun platform 1.0. This affects the function AttributeCategoryController of the file /attributecategory/queryAll. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2025-10457	The function responsible for handling BLE connection responses does not verify whether a response is expected—that is, whether the device has initiated a connection request. Instead, it relies solely on identifier matching.	4.3	More Details
CVE-2025-10676	A weakness has been identified in fuyang_lipengjun platform 1.0. Affected is the function BrandController of the file /brand/queryAll. Executing manipulation can lead to improper authorization. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-10675	A security flaw has been discovered in fuyang_lipengjun platform 1.0. This impacts the function AttributeController of the file /attribute/queryAll. Performing manipulation results in improper authorization. Remote exploitation of the attack is possible. The exploit has been released to the public and may be	4.3	More Details

	exploited.		
CVE-2025-57914	Cross-Site Request Forgery (CSRF) vulnerability in Matat Technologies Deliver via Shipos for WooCommerce allows Cross Site Request Forgery. This issue affects Deliver via Shipos for WooCommerce: from n/a through 3.0.2.	4.3	More Details
CVE-2025-59801	In Artifex GhostXPS before 10.06.0, there is a stack-based buffer overflow in xps_unpredict_tiff in xpstiff.c because the samplesperpixel value is not checked.	4.3	More Details
CVE-2025-59800	In Artifex Ghostscript through 10.05.1, ocr_begin_page in devices/gdevpdfocr.c has an integer overflow that leads to a heap-based buffer overflow in ocr_line8.	4.3	More Details
CVE-2025-57915	Cross-Site Request Forgery (CSRF) vulnerability in César Martín TOCHAT.BE allows Cross Site Request Forgery. This issue affects TOCHAT.BE: from n/a through 1.3.4.	4.3	More Details
CVE-2025-59798	Artifex Ghostscript through 10.05.1 has a stack-based buffer overflow in pdf_write_cmap in devices/vector/gdevpdtw.c.	4.3	More Details
CVE-2025-58663	Missing Authorization vulnerability in Themeum Qubely allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Qubely: from n/a through 1.8.14.	4.3	More Details
CVE-2025-58664	Missing Authorization vulnerability in Azizul Hasan Text To Speech TTS Accessibility allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Text To Speech TTS Accessibility: from n/a through 1.9.20.	4.3	More Details
CVE-2025-58666	Missing Authorization vulnerability in Kommo Website Chat Button: Kommo integration allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Website Chat Button: Kommo integration: from n/a through 1.3.1.	4.3	More Details
CVE-2025-58668	Missing Authorization vulnerability in VibeThemes WPLMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WPLMS : from n/a through 4.970.	4.3	More Details
CVE-2025-10766	A weakness has been identified in SeriaWei ZKEACMS up to 4.3. This issue affects the function Download of the file EventViewerController.cs. Executing manipulation of the argument ID can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10614	A vulnerability was determined in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0 on COVID. This affects an unknown function of the file /print_reports_prev.php. Executing manipulation of the argument profile_id can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2025-59455	In JetBrains TeamCity before 2025.07.2 project isolation bypass was possible due to race condition	4.2	More Details
CVE-2025-35434	CISA Thorium does not validate TLS certificates when connecting to Elasticsearch. An unauthenticated attacker with access to a Thorium cluster could impersonate the Elasticsearch service. Fixed in 1.1.2.	4.2	More Details
CVE-2025-0875	Authorization Bypass Through User-Controlled Key vulnerability in PROLIZ Computer Software Hardware Service Trade Ltd. Co. OBS (Student Affairs Information System) allows Parameter Injection.This issue affects OBS (Student Affairs Information System): before v26.0328.	4.2	More Details
CVE-2025-54855	Cleartext storage of sensitive information was discovered in Click Programming Software version v3.60. The vulnerability can be exploited by a local user with access to the file system, while an administrator session is active, to steal credentials stored in clear text.	4.2	More Details
CVE-2025-55904	Open5GS v2.7.5, prior to commit 67ba7f92bbd7a378954895d96d9d7b05d5b64615, is vulnerable to a NULL pointer dereference when a multipart/related HTTP POST request with an empty HTTP body is sent to the SBI of either AMF, AUSF, BSF, NRF, NSSF, PCF, SMF, UDM, or UDR, resulting in a denial of service. This occurs in the parse_multipart function in lib/sbi/message.c.	4.0	More Details
CVE-2025-58012	Authorization Bypass Through User-Controlled Key vulnerability in Alex Content Mask allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Content Mask: from n/a through 1.8.5.2.	3.8	More Details
CVE-	Missing Authorization vulnerability in codepeople CP Multi View Event Calendar allows Exploiting Incorrectly		

2025-58009	Configured Access Control Security Levels. This issue affects CP Multi View Event Calendar : from n/a through 1.4.32.	3.8	More Details
CVE-2025-30187	In some circumstances, when DNSdist is configured to use the nghttp2 library to process incoming DNS over HTTPS queries, an attacker might be able to cause a denial of service by crafting a DoH exchange that triggers an unbounded I/O read loop, causing an unexpected consumption of CPU resources.	3.7	More Details
CVE-2017-20200	A vulnerability has been found in Coinomi up to 1.7.6. This issue affects some unknown processing. Such manipulation leads to cleartext transmission of sensitive information. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit has been disclosed to the public and may be used. The vendor replied with: "(...) there isn't any security implication associated with your findings."	3.7	More Details
CVE-2025-59410	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the code in the scheduler for downloading a tiny file is hard coded to use the HTTP protocol, rather than HTTPS. This means that an attacker could perform a Man-in-the-Middle attack, changing the network request so that a different piece of data gets downloaded. This vulnerability is fixed in 2.1.0.	3.7	More Details
CVE-2025-10761	A vulnerability has been found in Harness 3.3.0. Affected is an unknown function of the file /api/v1/login of the component Login Endpoint. The manipulation leads to improper restriction of excessive authentication attempts. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-10776	A vulnerability was detected in LionCoders SalePro POS up to 5.5.0. This issue affects some unknown processing of the component Login. Performing manipulation results in cleartext transmission of sensitive information. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-59692	PureVPN client applications on Linux through September 2025 mishandle firewalling. They flush the system's existing iptables rules and apply default ACCEPT policies when connecting to a VPN server. This removes firewall rules that may have been configured manually or by other software (e.g., UFW, container engines, or system security policies). Upon VPN disconnect, the original firewall state is not restored. As a result, the system may become unintentionally exposed to network traffic that was previously blocked. This affects CLI 2.0.1 and GUI 2.10.0.	3.7	More Details
CVE-2025-10671	A vulnerability has been found in youth-is-as-pale-as-poetry e-learning 1.0. Impacted is the function encryptSecret of the file e-learning-master\exam-api\src\main\java\com\yf\exam\ability\shiro\jwt\JwtUtils.java of the component JWT Token Handler. The manipulation leads to insufficiently random values. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used.	3.7	More Details
CVE-2025-59691	PureVPN client applications on Linux through September 2025 allow IPv6 traffic to leak outside the VPN tunnel upon network events such as Wi-Fi reconnect or system resume. In the CLI client, the VPN auto-reconnects and claims to be connected, but IPv6 traffic is no longer routed or blocked. In the GUI client, the IPv6 connection remains functional after disconnection until the user clicks Reconnect. In both cases, the real IPv6 address is exposed to external services, violating user privacy and defeating the advertised IPv6 leak protection. This affects CLI 2.0.1 and GUI 2.10.0.	3.7	More Details
CVE-2025-4444	A security flaw has been discovered in Tor up to 0.4.7.16/0.4.8.17. Impacted is an unknown function of the component Onion Service Descriptor Handler. Performing manipulation results in resource consumption. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is considered difficult. Upgrading to version 0.4.8.18 and 0.4.9.3-alpha is recommended to address this issue. It is recommended to upgrade the affected component.	3.7	More Details
CVE-2025-10837	A security vulnerability has been detected in code-projects Simple Food Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /ordersimple/order.php. The manipulation of the argument ID leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2025-10591	A weakness has been identified in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /intranet/educar_funcao_cad.php of the component Editar Função Page. This manipulation of the argument abreviatura/tipoacao causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	3.5	More Details
CVE-2025-10584	A vulnerability was identified in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /intranet/educar_calendario_anotacao_cad.php. Such manipulation of the argument nm_anotacao/descricao leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	3.5	More Details

CVE-2025-10631	A vulnerability was identified in itsourcecode Online Petshop Management System 1.0. Impacted is an unknown function of the file addcnp.php of the component Available Products Page. The manipulation of the argument name/description leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2025-10632	A security flaw has been discovered in itsourcecode Online Petshop Management System 1.0. The affected element is an unknown function of the file availableframe.php of the component Admin Dashboard. The manipulation of the argument name/address results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	3.5	More Details
CVE-2025-10642	A vulnerability has been found in wangchenyi1996 chat_forum up to 80bdb92f5b460d36cab36e530a2c618acef5afd2. This impacts an unknown function of the file /q.php. Such manipulation of the argument path leads to cross site scripting. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	3.5	More Details
CVE-2025-0672	An authentication bypass vulnerability exists in multiple WSO2 products when FIDO authentication is enabled. When a user account is deleted, the system does not automatically remove associated FIDO registration data. If a new user account is later created using the same username, the system may associate the new account with the previously registered FIDO device. This flaw may allow a previously deleted user to authenticate using their FIDO credentials and impersonate the newly created user, resulting in unauthorized access. The vulnerability applies only to deployments that utilize FIDO-based authentication.	3.3	More Details
CVE-2025-10823	A vulnerability was found in axboe fio up to 3.41. This affects the function str_buffer_pattern_cb of the file options.c. Performing manipulation results in null pointer dereference. The attack must be initiated from a local position. The exploit has been made public and could be used.	3.3	More Details
CVE-2025-59349	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, DragonFly2 uses the os.MkdirAll function to create certain directory paths with specific access permissions. This function does not perform any permission checks when a given directory path already exists. This allows a local attacker to create a directory to be used later by DragonFly2 with broad permissions before DragonFly2 does so, potentially allowing the attacker to tamper with the files. This vulnerability is fixed in 2.1.0.	3.3	More Details
CVE-2025-9081	Mattermost versions 10.5.x <= 10.5.8, 9.11.x <= 9.11.17 fail to properly validate access controls which allows any authenticated user to download sensitive files via board file download endpoint using UUID enumeration	3.1	More Details
CVE-2025-59414	Nuxt is an open-source web development framework for Vue.js. Prior to 3.19.0 and 4.1.0, A client-side path traversal vulnerability in Nuxt's Island payload revival mechanism allowed attackers to manipulate client-side requests to different endpoints within the same application domain when specific prerendering conditions are met. The vulnerability occurs in the client-side payload revival process (revive-payload.client.ts) where Nuxt Islands are automatically fetched when encountering serialized __nuxt_island objects. During prerendering, if an API endpoint returns user-controlled data containing a crafted __nuxt_island object, he data gets serialized with devalue.stringify and stored in the prerendered page. When a client navigates to the prerendered page, devalue.parse deserializes the payload. The Island reviver attempts to fetch /__nuxt_island/${key}.json where key could contain path traversal sequences. Update to Nuxt 3.19.0+ or 4.1.0+.	3.1	More Details
CVE-2025-10778	A vulnerability has been found in Smartstore up to 6.2.0. The affected element is an unknown function of the file /checkout/confirm/ of the component Gift Voucher Handler. The manipulation leads to race condition. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is described as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-10758	A security vulnerability has been detected in htmly up to 3.1.0. The impacted element is an unknown function of the file /htmly/admin/field/post of the component Custom Field Handler. Such manipulation of the argument label leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-59546	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, administrators and content editors can set html in module titles that could include javascript which could be used for XSS based attacks. This issue has been patched in version 10.1.0.	2.4	More Details
CVE-2025-34194	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (Windows client deployments) contain an insecure temporary-file handling vulnerability in the PrinterInstallerClient components. The software creates files as NT AUTHORITY\SYSTEM inside a directory under the control of the local user (C:\Users\%USER%\AppData\Local\Temp\). An attacker who can place symbolic links or otherwise influence filenames in that directory can cause the service to follow the link and write to arbitrary filesystem locations as SYSTEM. This allows a local, unprivileged user to overwrite or create files as SYSTEM, leading to local privilege escalation and the ability to modify configuration files, replace or inject binaries, or otherwise compromise confidentiality, integrity, and availability of the system. NOTE: This vulnerability has been addressed, but an affected version range is not yet fully determined. This record will be updated when the	N/A	More Details

	vendor provides confirmed version information.		
CVE-2025-59532	Codex CLI is a coding agent from OpenAI that runs locally. In versions 0.2.0 to 0.38.0, due to a bug in the sandbox configuration logic, Codex CLI could treat a model-generated cwd as the sandbox's writable root, including paths outside of the folder where the user started their session. This logic bypassed the intended workspace boundary and enables arbitrary file writes and command execution where the Codex process has permissions - this did not impact the network-disabled sandbox restriction. This issue has been patched in Codex CLI 0.39.0 that canonicalizes and validates that the boundary used for sandbox policy is based on where the user started the session, and not the one generated by the model. Users running 0.38.0 or earlier should update immediately via their package manager or by reinstalling the latest Codex CLI to ensure sandbox boundaries are enforced. If using the Codex IDE extension, users should immediately update to 0.4.12 for a fix of the sandbox issue.	N/A	More Details
CVE-2023-53337	In the Linux kernel, the following vulnerability has been resolved: nilfs2: do not write dirty data after degenerating to read-only According to syzbot's report, mark_buffer_dirty() called from nilfs_segctor_do_construct() outputs a warning with some patterns after nilfs2 detects metadata corruption and degrades to read-only mode. After such read-only degeneration, page cache data may be cleared through nilfs_clear_dirty_page() which may also clear the uptodate flag for their buffer heads. However, even after the degeneration, log writes are still performed by unmount processing etc., which causes mark_buffer_dirty() to be called for buffer heads without the "uptodate" flag and causes the warning. Since any writes should not be done to a read-only file system in the first place, this fixes the warning in mark_buffer_dirty() by letting nilfs_segctor_do_construct() abort early if in read-only mode. This also changes the retry check of nilfs_segctor_write_out() to avoid unnecessary log write retries if it detects -EROFS that nilfs_segctor_do_construct() returned.	N/A	More Details
CVE-2023-53336	In the Linux kernel, the following vulnerability has been resolved: media: ipu-bridge: Fix null pointer deref on SSDB/PLD parsing warnings When ipu_bridge_parse_rotation() and ipu_bridge_parse_orientation() run sensor->adev is not set yet. So if either of the dev_warn() calls about unknown values are hit this will lead to a NULL pointer deref. Set sensor->adev earlier, with a borrowed ref to avoid making unrolling on errors harder, to fix this.	N/A	More Details
CVE-2023-53335	In the Linux kernel, the following vulnerability has been resolved: RDMA/cxgb4: Fix potential null-ptr-deref in pass_establish() If get_ep_from_tid() fails to lookup non-NULL value for ep, ep is dereferenced later regardless of whether it is empty. This patch adds a simple sanity check to fix the issue. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-47910	When using http.CrossOriginProtection, the AddInsecureBypassPattern method can unexpectedly bypass more requests than intended. CrossOriginProtection then skips validation, but forwards the original request path, which may be served by a different handler without the intended security protections.	N/A	More Details
CVE-2025-57204	Stocky POS with Inventory Management & HRM (ui-lib) version 5.0 is affected by a Stored Cross-Site Scripting (XSS) vulnerability within the Products module available to authenticated users. The vulnerability resides in the product name parameter submitted to the product-creation endpoint via a standard POST form. Due to insufficient input sanitization and output encoding, attackers can inject HTML/JS payloads. The payload is stored and subsequently rendered unsanitized in downstream views, leading to JavaScript execution in other users' browsers when they access the affected product pages. This issue allows an authenticated attacker to execute arbitrary JavaScript in the context of another user, potentially enabling session hijacking, privilege escalation within the application, data exfiltration, or administrative account takeover. The application also lacks a restrictive Content Security Policy (CSP), increasing exploitability.	N/A	More Details
CVE-2025-57205	iNiLabs School Express (SMS Express) 6.2 is affected by a Stored Cross-Site Scripting (XSS) vulnerability in the content-management features available to authenticated admin users. The vulnerability resides in POSTed editor parameters submitted to the /posts/edit/{id} endpoint (and similarly in Notice and Pages editors). Due to insufficient input sanitization and output encoding, attackers can inject HTML/JS payloads. The payload is saved and later rendered unsanitized, resulting in JavaScript execution in other users' browsers when they access the affected content. This issue allows an authenticated attacker to execute arbitrary JavaScript in the context of another user, potentially leading to session hijacking, privilege escalation, data exfiltration, or administrative account takeover. The application does not enforce a restrictive Content Security Policy (CSP) or adequate filtering to prevent such attacks.	N/A	More Details
CVE-2022-50374	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_{ldisc,serdev}: check percpu_init_rwsem() failure syzbot is reporting NULL pointer dereference at hci_uart_tty_close() [1], for rcu_sync_enter() is called without rcu_sync_init() due to hci_uart_tty_open() ignoring percpu_init_rwsem() failure. While we are at it, fix that hci_uart_register_device() ignores percpu_init_rwsem() failure and hci_uart_unregister_device() does not call percpu_free_rwsem().	N/A	More Details
CVE-2025-34192	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.893 and Application versions prior to 20.0.2140 (macOS/Linux client deployments) are built against OpenSSL 1.0.2h-fips (released May 2016), which has been end-of-life since 2019 and is no longer supported by the OpenSSL project. Continued use of this outdated cryptographic library exposes deployments to known vulnerabilities that are no longer patched, weakening the overall security posture. Affected daemons may emit deprecation warnings and rely	N/A	More Details

	on cryptographic components with unresolved security flaws, potentially enabling attackers to exploit weaknesses in TLS/SSL processing or cryptographic operations.		
CVE-2022-50373	In the Linux kernel, the following vulnerability has been resolved: fs: dlm: fix race in lowcomms This patch fixes a race between queue_work() in _dlm_lowcomms_commit_msg() and srcu_read_unlock(). The queue_work() can take the final reference of a dlm_msg and so msg->idx can contain garbage which is signaled by the following warning: [676.237050] ------------[cut here]------------ [676.237052] WARNING: CPU: 0 PID: 1060 at include/linux/srcu.h:189 dlm_lowcomms_commit_msg+0x41/0x50 [676.238945] Modules linked in: dlm_locktorture torture rpcsec_gss_krb5 intel_rapl_msr intel_rapl_common iTCO_wdt iTCO_vendor_support qxl kvm_intel drm_ttm_helper vmw_vsock_virtio_transport kvm vmw_vsock_virtio_transport_common ttm irqbypass crc32_pclmul joydev crc32c_intel serio_raw drm_kms_helper vsock virtio_scsi virtio_console virtio_balloon snd_pcm drm syscopyarea sysfillrect sysimgblt snd_timer fb_sys_fops i2c_i801 lpc_ich snd i2c_smbus soundcore pcspkr [676.244227] CPU: 0 PID: 1060 Comm: lock_torture_wr Not tainted 5.19.0-rc3+ #1546 [676.245216] Hardware name: Red Hat KVM/RHEL-AV, BIOS 1.16.0-2.module+el8.7.0+15506+033991b0 04/01/2014 [676.246460] RIP: 0010:dlm_lowcomms_commit_msg+0x41/0x50 [676.247132] Code: fe ff ff ff 75 24 48 c7 c6 bd 0f 49 bb 48 c7 c7 38 7c 01 bd e8 00 e7 ca ff 89 de 48 c7 c7 60 78 01 bd e8 42 3d cd ff 5b 5d c3 <0f> 0b eb d8 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 55 48 [676.249253] RSP: 0018:ffffa401c18ffc68 EFLAGS: 00010282 [676.249855] RAX: 0000000000000001 RBX: 00000000ffff8b76 RCX: 0000000000000006 [676.250713] RDX: 0000000000000000 RSI: ffffffffbccf3a10 RDI: ffffffffbcc7b62e [676.251610] RBP: ffffa401c18ffc70 R08: 0000000000000001 R09: 0000000000000001 [676.252481] R10: 0000000000000001 R11: 0000000000000001 R12: 0000000000000005 [676.253421] R13: ffff8b76786ec370 R14: ffff8b76786ec370 R15: ffff8b76786ec480 [676.254257] FS: 0000000000000000(0000) GS:ffff8b7777800000(0000) knlGS:0000000000000000 [676.255239] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [676.255897] CR2: 00005590205d88b8 CR3: 000000017656c003 CR4: 0000000000770ee0 [676.256734] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [676.257567] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [676.258397] PKRU: 55555554 [676.258729] Call Trace: [676.259063] <TASK> [676.259354] dlm_midcomms_commit_mhandle+0xcc/0x110 [676.259964] queue_bast+0x8b/0xb0 [676.260423] grant_pending_locks+0x166/0x1b0 [676.261007] _unlock_lock+0x75/0x90 [676.261469] unlock_lock.isra.57+0x62/0xa0 [676.262009] dlm_unlock+0x21e/0x330 [676.262457] ? lock_torture_stats+0x80/0x80 [dlm_locktorture] [676.263183] torture_unlock+0x5a/0x90 [dlm_locktorture] [676.263815] ? preempt_count_sub+0xba/0x100 [676.264361] ? complete+0x1d/0x60 [676.264777] lock_torture_writer+0xb8/0x150 [dlm_locktorture] [676.265555] kthread+0x10a/0x130 [676.266007] ? kthread_complete_and_exit+0x20/0x20 [676.266616] ret_from_fork+0x22/0x30 [676.267097] </TASK> [676.267381] irq event stamp: 9579855 [676.267824] hardirqs last enabled at (9579863): [<ffffffffbb14e6f8>] __up_console_sem+0x58/0x60 [676.268896] hardirqs last disabled at (9579872): [<ffffffffbb14e6dd>] __up_console_sem+0x3d/0x60 [676.270008] softirqs last enabled at (9579798): [<ffffffffbc200349>] __do_softirq+0x349/0x4c7 [676.271438] softirqs last disabled at (9579897): [<ffffffffbb0d54c0>] irq_exit_rcu+0xb0/0xf0 [676.272796] ---[end trace 0000000000000000]--- I reproduced this warning with dlm_locktorture test which is currently not upstream. However this patch fix the issue by make a additional refcount between dlm_lowcomms_new_msg() and dlm_lowcomms_commit_msg(). In case of the race the kref_put() in dlm_lowcomms_commit_msg() will be the final put.	N/A	More Details
CVE-2022-50372	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix memory leak when build ntlmssp negotiate blob failed There is a memory leak when mount cifs: unreferenced object 0xffff888166059600 (size 448): comm "mount.cifs", pid 51391, jiffies 4295596373 (age 330.596s) hex dump (first 32 bytes): fe 53 4d 42 40 00 00 00 00 00 00 00 01 00 82 00 .SMB@..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<0000000060609a61>] mempool_alloc+0xe1/0x260 [<00000000adfa6c63>] cifs_small_buf_get+0x24/0x60 [<00000000ebb404c7>] __smb2_plain_req_init+0x32/0x460 [<00000000bcf875b4>] SMB2_sess_alloc_buffer+0xa4/0x3f0 [<00000000753a2987>] SMB2_sess_auth_rawntlmssp_negotiate+0xf5/0x480 [<00000000f0c1f4f9>] SMB2_sess_setup+0x253/0x410 [<00000000a8b83303>] cifs_setup_session+0x18f/0x4c0 [<00000000854bd16d>] cifs_get_smb_ses+0xae7/0x13c0 [<000000006cbc43d9>] mount_get_conns+0x7a/0x730 [<000000005922d816>] cifs_mount+0x103/0xd10 [<00000000e33def3b>] cifs_smb3_do_mount+0x1dd/0xc90 [<0000000078034979>] smb3_get_tree+0x1d5/0x300 [<000000004371f980>] vfs_get_tree+0x41/0xf0 [<00000000b670d8a7>] path_mount+0x9b3/0xdd0 [<000000005e839a7d>] __x64_sys_mount+0x190/0x1d0 [<000000009404c3b9>] do_syscall_64+0x35/0x80 When build ntlmssp negotiate blob failed, the session setup request should be freed.	N/A	More Details
CVE-2025-43806	Batch Engine in Liferay Portal 7.4.0 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.7, 2023.Q3.1 through 2023.Q3.10, and 7.4 GA through update 92 does not properly check permission with import and export tasks, which allows remote authenticated users to access the exported data via the REST APIs.	N/A	More Details
CVE-2025-	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application include Windows client components (PrinterInstallerClientInterface.exe, PrinterInstallerClient.exe, PrinterInstallerClientLauncher.exe) that lack modern compile-time and runtime exploit mitigations and rely on outdated runtimes. These binaries are built as 32-bit, without Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Control Flow Guard (CFG), or stack-protection, and they incorporate legacy technologies (Pascal/Delphi and Python 2) which are no longer commonly maintained. Several of these processes run with elevated privileges	N/A	More

34193	(NT AUTHORITY\SYSTEM for PrinterInstallerClient.exe and PrinterInstallerClientLauncher.exe), and the client automatically downloads and installs printer drivers. The absence of modern memory safety mitigations and the use of unmaintained runtimes substantially increase the risk that memory-corruption or other exploit primitives — for example from crafted driver content or maliciously crafted inputs — can be turned into remote or local code execution and privilege escalation to SYSTEM.		Details
CVE-2025-34197	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.951, Application prior to 20.0.2368 (VA and SaaS deployments) contain an undocumented local user account named ubuntu with a preset password and a sudoers entry granting that account passwordless root privileges (ubuntu ALL=(ALL) NOPASSWD: ALL). Anyone who knows the hardcoded password can obtain root privileges via local console or equivalent administrative access, enabling local privilege escalation. NOTE: The patch for this vulnerability is reported to be incomplete: /etc/shadow was remediated but /etc/sudoers remains vulnerable.	N/A	More Details
CVE-2025-34195	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 1.0.735 and Application prior to 20.0.1330 (Windows client deployments) contain a remote code execution vulnerability during driver installation caused by unquoted program paths. The PrinterInstallerClient driver-installation component launches programs using an unquoted path under "C:\Program Files (x86)\Printer Properties Pro\Printer Installer". Because the path is unquoted, the operating system may execute a program located at a short-path location such as C:\Program.exe before the intended binaries in the quoted path. If an attacker can place or cause a program to exist at that location, it will be executed with the privileges of the installer process (which may be elevated), enabling arbitrary code execution and potential privilege escalation. This weakness can be used to achieve remote code execution and full compromise of affected Windows endpoints.	N/A	More Details
CVE-2025-43814	In Liferay Portal 7.4.0 through 7.4.3.112, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions the audit events records a user’s password reminder answer, which allows remote authenticated users to obtain a user’s password reminder answer via the audit events.	N/A	More Details
CVE-2025-43810	Insecure Direct Object Reference (IDOR) vulnerability with commerce order notes in Liferay Portal 7.3.5 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, and 7.4 GA through update 92 allows remote authenticated users to from one virtual instance to add a note to an order in a different virtual instance via the _com_liferay_commerce_order_web_internal_portlet_CommerceOrderPortlet_commerceOrderId parameter.	N/A	More Details
CVE-2022-50369	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix null-ptr-deref in vkms_release() A null-ptr-deref is triggered when it tries to destroy the workqueue in vkms->output.composer_workq in vkms_release(). KASAN: null-ptr-deref in range [0x0000000000000118-0x000000000000011f] CPU: 5 PID: 17193 Comm: modprobe Not tainted 6.0.0-11331-gd465bff130bf #24 RIP: 0010:destroy_workqueue+0x2f/0x710 ... Call Trace: <TASK> ? vkms_config_debugfs_init+0x50/0x50 [vkms] __devm_drm_dev_alloc+0x15a/0x1c0 [drm] vkms_init+0x245/0x1000 [vkms] do_one_initcall+0xd0/0x4f0 do_init_module+0x1a4/0x680 load_module+0x6249/0x7110 __do_sys_finit_module+0x140/0x200 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 The reason is that an OOM happened which triggers the destroy of the workqueue, however, the workqueue is alloced in the later process, thus a null-ptr-deref happened. A simple call graph is shown as below: vkms_init() vkms_create() devm_drm_dev_alloc() __devm_drm_dev_alloc() devm_drm_dev_init() devm_add_action_or_reset() devm_add_action() # an error happened devm_drm_dev_init_release() drm_dev_put() kref_put() drm_dev_release() vkms_release() destroy_workqueue() # null-ptr-deref happened vkms_modeset_init() vkms_output_init() vkms_crtc_init() # where the workqueue get allocated Fix this by checking if composer_workq is NULL before passing it to the destroy_workqueue() in vkms_release().	N/A	More Details
CVE-2022-50371	In the Linux kernel, the following vulnerability has been resolved: led: qcom-lpg: Fix sleeping in atomic lpg_brighness_set() function can sleep, while led's brightness_set() callback must be non-blocking. Change LPG driver to use brightness_set_blocking() instead. BUG: sleeping function called from invalid context at kernel/locking/mutex.c:580 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 0, name: swapper/0 preempt_count: 101, expected: 0 INFO: lockdep is turned off. CPU: 0 PID: 0 Comm: swapper/0 Tainted: G W 6.1.0-rc1-00014-gbe99b089c6fc-dirty #85 Hardware name: Qualcomm Technologies, Inc. DB820c (DT) Call trace: dump_backtrace.part.0+0xe4/0xf0 show_stack+0x18/0x40 dump_stack_lvl+0x88/0xb4 dump_stack+0x18/0x34 __might_resched+0x170/0x254 __might_sleep+0x48/0x9c __mutex_lock+0x4c/0x400 mutex_lock_nested+0x2c/0x40 lpg_brightness_single_set+0x40/0x90 led_set_brightness_nosleep+0x34/0x60 led_heartbeat_function+0x80/0x170 call_timer_fn+0xb8/0x340 __run_timers.part.0+0x20c/0x254 run_timer_softirq+0x3c/0x7c _stext+0x14c/0x578 ____do_softirq+0x10/0x20 call_on_irq_stack+0x2c/0x5c do_softirq_own_stack+0x1c/0x30 __irq_exit_rcu+0x164/0x170 irq_exit_rcu+0x10/0x40 el1_interrupt+0x38/0x50 el1h_64_irq_handler+0x18/0x2c el1h_64_irq+0x64/0x68 cpuidle_enter_state+0xc8/0x380 cpuidle_enter+0x38/0x50 do_idle+0x244/0x2d0 cpu_startup_entry+0x24/0x30 rest_init+0x128/0x1a0 arch_post_acpi_subsys_init+0x0/0x18 start_kernel+0x6f4/0x734 __primary_switched+0xbc/0xc4	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: dmaengine: hisilicon: Add multi-thread support for a DMA channel When we get a DMA channel and try to use it in multiple threads it will cause oops and hanging the system. % echo 100 > /sys/module/dmatest/parameters/threads_per_chan % echo 100 >		

CVE-2022-50362	/sys/module/dmatest/parameters/iterations % echo 1 > /sys/module/dmatest/parameters/run [383493.327077] Unable to handle kernel paging request at virtual address dead000000000108 [383493.335103] Mem abort info: [383493.335103] ESR = 0x96000044 [383493.335105] EC = 0x25: DABT (current EL), IL = 32 bits [383493.335107] SET = 0, FnV = 0 [383493.335108] EA = 0, S1PTW = 0 [383493.335109] FSC = 0x04: level 0 translation fault [383493.335110] Data abort info: [383493.335111] ISV = 0, ISS = 0x00000044 [383493.364739] CM = 0, WnR = 1 [383493.367793] [dead000000000108] address between user and kernel address ranges [383493.375021] Internal error: Oops: 96000044 [#1] PREEMPT SMP [383493.437574] CPU: 63 PID: 27895 Comm: dma0chan0-copy2 Kdump: loaded Tainted: GO 5.17.0-rc4+ #2 [383493.457851] pstate: 204000c9 (nzCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [383493.465331] pc : vchan_tx_submit+0x64/0xa0 [383493.469957] lr : vchan_tx_submit+0x34/0xa0 This occurs because the transmission timed out, and that's due to data race. Each thread rewrite channels's descriptor as soon as device_issue_pending is called. It leads to the situation that the driver thinks that it uses the right descriptor in interrupt handler while channels's descriptor has been changed by other thread. The descriptor which in fact reported interrupt will not be handled any more, as well as its tx->callback. That's why timeout reports. With current fixes channels' descriptor changes it's value only when it has been used. A new descriptor is acquired from vc->desc_issued queue that is already filled with descriptors that are ready to be sent. Threads have no direct access to DMA channel descriptor. In case of channel's descriptor is busy, try to submit to HW again when a descriptor is completed. In this case, vc->desc_issued may be empty when hisi_dma_start_transfer is called, so delete error reporting on this. Now it is just possible to queue a descriptor for further processing.	N/A	More Details
CVE-2025-59881	Rejected reason: Not used	N/A	More Details
CVE-2025-59880	Rejected reason: Not used	N/A	More Details
CVE-2025-59879	Rejected reason: Not used	N/A	More Details
CVE-2025-59878	Rejected reason: Not used	N/A	More Details
CVE-2025-59877	Rejected reason: Not used	N/A	More Details
CVE-2025-59876	Rejected reason: Not used	N/A	More Details
CVE-2025-59813	Rejected reason: Not used	N/A	More Details
CVE-2025-59812	Rejected reason: Not used	N/A	More Details
CVE-2025-59811	Rejected reason: Not used	N/A	More Details
CVE-2022-50363	In the Linux kernel, the following vulnerability has been resolved: skmsg: pass gfp argument to alloc_sk_msg() syzbot found that alloc_sk_msg() could be called from a non sleepable context. sk_psock_verdict_recv() uses rcu_read_lock() protection. We need the callers to pass a gfp_t argument to avoid issues. syzbot report was: BUG: sleeping function called from invalid context at include/linux/sched/mm.h:274 in_atomic(): 0, irqs_disabled(): 0, non_block: 0, pid: 3613, name: syz-executor414 preempt_count: 0, expected: 0 RCU nest depth: 1, expected: 0 INFO: lockdep is turned off. CPU: 0 PID: 3613 Comm: syz-executor414 Not tainted 6.0.0-syzkaller-09589-g55be6084c8e0 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/22/2022 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1e3/0x2cb lib/dump_stack.c:106 __might_resched+0x538/0x6a0 kernel/sched/core.c:9877 might_alloc include/linux/sched/mm.h:274 [inline] slab_pre_alloc_hook mm/slab.h:700 [inline] slab_alloc_node mm/slub.c:3162 [inline] slab_alloc mm/slub.c:3256 [inline] kmem_cache_alloc_trace+0x59/0x310 mm/slub.c:3287 kmalloc include/linux/slab.h:600 [inline] kzalloc include/linux/slab.h:733 [inline] alloc_sk_msg net/core/skmsg.c:507 [inline] sk_psock_skb_ingress_self+0x5c/0x330 net/core/skmsg.c:600 sk_psock_verdict_apply+0x395/0x440 net/core/skmsg.c:1014 sk_psock_verdict_recv+0x34d/0x560 net/core/skmsg.c:1201	N/A	More Details

	tcp_read_skb+0x4a1/0x790 net/ipv4/tcp.c:1770 tcp_rcv_established+0x129d/0x1a10 net/ipv4/tcp_input.c:5971 tcp_v4_do_rcv+0x479/0xac0 net/ipv4/tcp_ipv4.c:1681 sk_backlog_rcv include/net/sock.h:1109 [inline] __release_sock+0x1d8/0x4c0 net/core/sock.c:2906 release_sock+0x5d/0x1c0 net/core/sock.c:3462 tcp_sendmsg+0x36/0x40 net/ipv4/tcp.c:1483 sock_sendmsg_nosec net/socket.c:714 [inline] sock_sendmsg net/socket.c:734 [inline] __sys_sendto+0x46d/0x5f0 net/socket.c:2117 __do_sys_sendto net/socket.c:2129 [inline] __se_sys_sendto net/socket.c:2125 [inline] __x64_sys_sendto+0xda/0xf0 net/socket.c:2125 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x2b/0x70 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd		
CVE-2022-50370	In the Linux kernel, the following vulnerability has been resolved: i2c: designware: Fix handling of real but unexpected device interrupts Commit c7b79a752871 ("mfd: intel-lpss: Add Intel Alder Lake PCH-S PCI IDs") caused a regression on certain Gigabyte motherboards for Intel Alder Lake-S where system crashes to NULL pointer dereference in i2c_dw_xfer_msg() when system resumes from S3 sleep state ("deep"). I was able to debug the issue on Gigabyte Z690 AORUS ELITE and made following notes: - Issue happens when resuming from S3 but not when resuming from "s2idle" - PCI device 00:15.0 == i2c_designware.0 is already in D0 state when system enters into pci_pm_resume_noirq() while all other i2c_designware PCI devices are in D3. Devices were runtime suspended and in D3 prior entering into suspend - Interrupt comes after pci_pm_resume_noirq() when device interrupts are re-enabled - According to register dump the interrupt really comes from the i2c_designware.0. Controller is enabled, I2C target address register points to a one detectable I2C device address 0x60 and the DW_IC_RAW_INTR_STAT register START_DET, STOP_DET, ACTIVITY and TX_EMPTY bits are set indicating completed I2C transaction. My guess is that the firmware uses this controller to communicate with an on-board I2C device during resume but does not disable the controller before giving control to an operating system. I was told the UEFI update fixes this but never the less it revealed the driver is not ready to handle TX_EMPTY (or RX_FULL) interrupt when device is supposed to be idle and state variables are not set (especially the dev->msgs pointer which may point to NULL or stale old data). Introduce a new software status flag STATUS_ACTIVE indicating when the controller is active in driver point of view. Now treat all interrupts that occur when is not set as unexpected and mask all interrupts from the controller.	N/A	More Details
CVE-2025-9495	The Vitogate 300 web interface fails to enforce proper server-side authentication and relies on frontend-based authentication controls. This allows an attacker to simply modify HTML elements in the browser’s developer tools to bypass login restrictions. By removing specific UI elements, an attacker can reveal the hidden administration menu, giving them full control over the device.	N/A	More Details
CVE-2025-9494	An OS command injection vulnerability has been discovered in the Vitogate 300, which can be exploited by malicious users to compromise affected installations. Specifically, the `/cgi-bin/vitogate.cgi` endpoint is affected, when the `form` JSON parameter is set to `form-0-2`. The vulnerability stems from the fact that that function at offset 0x21c24 does not properly sanitize supplied input before interpolating it into a format string which gets passed to `popen()`. Consequently, an authenticated attacker is able to inject arbitrary OS commands and thus gain code execution on affected devices.	N/A	More Details
CVE-2022-50364	In the Linux kernel, the following vulnerability has been resolved: i2c: mux: reg: check return value after calling platform_get_resource() It will cause null-ptr-deref in resource_size(), if platform_get_resource() returns NULL, move calling resource_size() after devm_ioremap_resource() that will check 'res' to avoid null-ptr-deref. And use devm_platform_get_and_ioremap_resource() to simplify code.	N/A	More Details
CVE-2025-34190	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (macOS/Linux client deployments) are vulnerable to an authentication bypass in PrinterInstallerClientService. The service requires root privileges for certain administrative operations, but these checks rely on calls to geteuid(). By preloading a malicious shared object overriding geteuid(), a local attacker can trick the service into believing it is running with root privileges. This bypass enables execution of administrative commands (e.g., enabling debug mode, managing configurations, or invoking privileged features) without proper authorization. While some actions requiring write access to protected files may still fail, the flaw effectively breaks the intended security model of the inter-process communication (IPC) system, allowing local attackers to escalate privileges and compromise system integrity. NOTE: This vulnerability has been addressed, but an affected version range is not yet fully determined. We will update this record as soon as the vendor provides confirmed version information.	N/A	More Details
CVE-2022-50365	In the Linux kernel, the following vulnerability has been resolved: skbuff: Account for tail adjustment during pull operations Extending the tail can have some unexpected side effects if a program uses a helper like BPF_FUNC_skb_pull_data to read partial content beyond the head skb headlen when all the skbs in the gso frag_list are linear with no head_frag - kernel BUG at net/core/skbuff.c:4219! pc : skb_segment+0xcf4/0xd2c lr : skb_segment+0x63c/0xd2c Call trace: skb_segment+0xcf4/0xd2c __udp_gso_segment+0xa4/0x544 udp4_ufo_fragment+0x184/0x1c0 inet_gso_segment+0x16c/0x3a4 skb_mac_gso_segment+0xd4/0x1b0 __skb_gso_segment+0xcc/0x12c udp_rcv_segment+0x54/0x16c udp_queue_rcv_skb+0x78/0x144 udp_unicast_rcv_skb+0x8c/0xa4 __udp4_lib_rcv+0x490/0x68c udp_rcv+0x20/0x30 ip_protocol_deliver_rcu+0x1b0/0x33c ip_local_deliver+0xd8/0x1f0 ip_rcv+0x98/0x1a4 deliver_ptype_list_skb+0x98/0x1ec __netif_receive_skb_core+0x978/0xc60 Fix this by marking these skbs as GSO_DODGY so segmentation can handle the tail updates accordingly.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: powercap: intel_rapl: fix UBSAN shift-out-of-		

CVE-2022-50366	bounds issue When value < time_unit, the parameter of ilog2() will be zero and the return value is -1. u64(-1) is too large for shift exponent and then will trigger shift-out-of-bounds: shift exponent 18446744073709551615 is too large for 32-bit type 'int' Call Trace: rapl_compute_time_window_core rapl_write_data_raw set_time_window store_constraint_time_window_us	N/A	More Details
CVE-2022-50367	In the Linux kernel, the following vulnerability has been resolved: fs: fix UAF/GPF bug in nilfs_mdt_destroy In alloc_inode, inode_init_always() could return -ENOMEM if security_inode_alloc() fails, which causes inode->i_private uninitialized. Then nilfs_is_metadata_file_inode() returns true and nilfs_free_inode() wrongly calls nilfs_mdt_destroy(), which frees the uninitialized inode->i_private and leads to crashes(e.g., UAF/GPF). Fix this by moving security_inode_alloc just prior to this_cpu_inc(nr_inodes)	N/A	More Details
CVE-2022-50368	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dsi: fix memory corruption with too many bridges Add the missing sanity check on the bridge counter to avoid corrupting data beyond the fixed-sized bridge array in case there are ever more than eight bridges. Patchwork: https://patchwork.freedesktop.org/patch/502668/	N/A	More Details
CVE-2025-34191	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.843 and Application prior to 20.0.1923 (macOS/Linux client deployments) contain an arbitrary file write vulnerability via the response file handling. When tasks produce output the service writes response data into files under /opt/PrinterInstallerClient/tmp/responses/ reusing the requested filename. The service follows symbolic links in the responses directory and writes as the service user (typically root), allowing a local, unprivileged user to cause the service to overwrite or create arbitrary files on the filesystem as root. This can be used to modify configuration files, replace or inject binaries or drivers, and otherwise achieve local privilege escalation and full system compromise.	N/A	More Details
CVE-2025-59526	mailgen is a Node.js package that generates responsive HTML e-mails for sending transactional mail. Prior to version 2.0.30, there is an HTML injection vulnerability in plaintext e-mails generated by Mailgen. Projects are affected if the Mailgen.generatePlaintext(email) method is used and given user-generated content. This vulnerability has been patched in version 2.0.30. A workaround involves stripping all HTML tags before passing any content into Mailgen.generatePlaintext(email).	N/A	More Details
CVE-2025-9960	A restriction bypass vulnerability in is-localhost-ip could allow attackers to perform Server-Side Request Forgery (SSRF). This issue affects is-localhost-ip: 2.0.0.	N/A	More Details
CVE-2025-34198	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.951 and Application prior to 20.0.2368 (VA and SaaS deployments) contain shared, hardcoded SSH host private keys in the appliance image. The same private host keys (RSA, ECDSA, and ED25519) are present across installations, rather than being uniquely generated per appliance. An attacker who obtains these private keys (for example from one compromised appliance image or another installation) can impersonate the appliance, decrypt or intercept SSH connections to appliances that use the same keys, and perform man-in-the-middle or impersonation attacks against administrative SSH sessions.	N/A	More Details
CVE-2025-59432	SCRAM (Salted Challenge Response Authentication Mechanism) is part of the family of Simple Authentication and Security Layer (SASL, RFC 4422) authentication mechanisms. Prior to version 3.2, a timing attack vulnerability exists in the SCRAM Java implementation. The issue arises because Arrays.equals was used to compare secret values such as client proofs and server signatures. Since Arrays.equals performs a short-circuit comparison, the execution time varies depending on how many leading bytes match. This behavior could allow an attacker to perform a timing side-channel attack and potentially infer sensitive authentication material. All users relying on SCRAM authentication are impacted. This vulnerability has been patched in version 3.1 by replacing Arrays.equals with MessageDigest.isEqual, which ensures constant-time comparison.	N/A	More Details
CVE-2025-34203	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.1002 and Application versions prior to 20.0.2614 (VA and SaaS deployments) contain multiple Docker containers that include outdated, end-of-life, unsupported, or otherwise vulnerable third-party components (examples: Nginx 1.17.x, OpenSSL 1.1.1d, various EOL Alpine/Debian/Ubuntu base images, and EOL Laravel/PHP libraries). These components are present across many container images and increase the product's attack surface, enabling exploitation chains when leveraged by an attacker. Multiple distinct EOL versions and unpatched libraries across containers; Nginx binaries date from 2019 in several images and Laravel versions observed include EOL releases (for example Laravel 5.5.x, 5.7.x, 5.8.x).	N/A	More Details
CVE-2025-34204	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (VA and SaaS deployments) contains multiple Docker containers that run primary application processes (for example PHP workers, Node.js servers and custom binaries) as the root user. This increases the blast radius of a container compromise and enables lateral movement and host compromise when a container is breached.	N/A	More Details
CVE-2023-53356	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_serial: Add null pointer check in gserial_suspend Consider a case where gserial_disconnect has already cleared gser->ioport. And if gserial_suspend gets called afterwards, it will lead to accessing of gser->ioport and thus causing null pointer dereference. Avoid this by adding a null pointer check. Added a static spinlock to prevent gser->ioport from becoming null after the newly added null pointer check.	N/A	More Details

CVE-2025-34205	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.843 and Application prior to 20.0.1923 (VA and SaaS deployments) contains dangerous PHP dead code present in multiple Docker-hosted PHP instances. A script named /var/www/app/resetroot.php (found in several containers) lacks authentication checks and, when executed, performs a SQL update that sets the database administrator username to 'root' and its password hash to the SHA-512 hash of the string 'password'. Separately, commented-out code in /var/www/app/lib/common/oses.php would unserialize session data (unserialize($_SESSION['osdata']))—a pattern that can enable remote code execution if re-enabled or reached with attacker-controlled serialized data. An attacker able to reach the resetroot.php endpoint can trivially reset the MySQL root password and obtain full database control; combined with deserialization issues this can lead to full remote code execution and system compromise.	N/A	More Details
CVE-2025-34206	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (VA and SaaS deployments) mount host configuration and secret material under /var/www/efs_storage into many Docker containers with overly-permissive filesystem permissions. Files such as secrets.env, GPG-encrypted blobs in .secrets, MySQL client keys, and application session files are accessible from multiple containers. An attacker who controls or reaches any container can read or modify these artifacts, leading to credential theft, RCE via Laravel APP_KEY, Portainer takeover, and full compromise.	N/A	More Details
CVE-2025-43803	Insecure direct object reference (IDOR) vulnerability in the Contacts Center widget in Liferay Portal 7.4.0 through 7.4.3.119, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.6, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows remote attackers to view contact information, including the contact’s name and email address, via the _com_liferay_contacts_web_portlet_ContactsCenterPortlet_entryId parameter.	N/A	More Details
CVE-2023-53357	In the Linux kernel, the following vulnerability has been resolved: md/raid10: check slab-out-of-bounds in md_bitmap_get_counter If we write a large number to md/bitmap_set_bits, md_bitmap_checkpage() will return -EINVAL because 'page >= bitmap->pages', but the return value was not checked immediately in md_bitmap_get_counter() in order to set *blocks value and slab-out-of-bounds occurs. Move check of 'page >= bitmap->pages' to md_bitmap_get_counter() and return directly if true.	N/A	More Details
CVE-2023-53358	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue under cocurrent smb2 tree disconnect There is UAF issue under cocurrent smb2 tree disconnect. This patch introduce TREE_CONN_EXPIRE flags for tcon to avoid cocurrent access.	N/A	More Details
CVE-2025-10568	HyperX NGENUITY software is potentially vulnerable to arbitrary code execution. HP is releasing updated software to address the potential vulnerability.	N/A	More Details
CVE-2023-53359	In the Linux kernel, the following vulnerability has been resolved: USB: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53360	In the Linux kernel, the following vulnerability has been resolved: NFSv4.2: Rework scratch handling for READ_PLUS (again) I found that the read code might send multiple requests using the same nfs_pgio_header, but nfs4_proc_read_setup() is only called once. This is how we ended up occasionally double-freeing the scratch buffer, but also means we set a NULL pointer but non-zero length to the xdr scratch buffer. This results in an oops the first time decoding needs to copy something to scratch, which frequently happens when decoding READ_PLUS hole segments. I fix this by moving scratch handling into the pageio read code. I provide a function to allocate scratch space for decoding read replies, and free the scratch buffer when the nfs_pgio_header is freed.	N/A	More Details
CVE-2023-53361	In the Linux kernel, the following vulnerability has been resolved: LoongArch: mm: Add p?d_leaf() definitions When I do LTP test, LTP test case ksm06 caused panic at break_ksm_pmd_entry -> pmd_leaf (Huge page table but False) -> pte_present (panic) The reason is pmd_leaf() is not defined, So like commit 501b81046701 ("mips: mm: add p?d_leaf() definitions") add p?d_leaf() definition for LoongArch.	N/A	More Details
CVE-2023-53362	In the Linux kernel, the following vulnerability has been resolved: bus: fsl-mc: don't assume child devices are all fsl-mc devices Changes in VFIO caused a pseudo-device to be created as child of fsl-mc devices causing a crash [1] when trying to bind a fsl-mc device to VFIO. Fix this by checking the device type when enumerating fsl-mc child devices. [1] Modules linked in: Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP CPU: 6 PID: 1289 Comm: sh Not tainted 6.2.0-rc5-00047-g7c46948a6e9c #2 Hardware name: NXP Layerscape LX2160ARDB (DT) pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mc_send_command+0x24/0x1f0 lr : dprc_get_obj_region+0xfc/0x1c0 sp : ffff80000a88b900 x29: ffff80000a88b900 x28: ffff48a9429e1400 x27: 00000000000002b2 x26: ffff48a9429e1718 x25: 0000000000000000 x24: 0000000000000000 x23: ffffd59331ba3918 x22: ffffd59331ba3000 x21: 0000000000000000 x20: ffff80000a88b9b8 x19: 0000000000000000 x18: 0000000000000001 x17: 7270642f636d2d6c x16: 73662e3030303030 x15: ffffffffffffffff x14: ffffd59330f1d668 x13: ffff48a8727dc389 x12: ffff48a8727dc386 x11: 0000000000000002 x10: 00008ceaf02f35d4 x9 : 0000000000000012 x8 : 0000000000000000 x7 : 0000000000000006 x6 : ffff80000a88bab0 x5 : 0000000000000000 x4 : 0000000000000000 x3 : ffff80000a88b9e8 x2 : ffff80000a88b9e8 x1 : 0000000000000000 x0 : ffff48a945142b80 Call trace: mc_send_command+0x24/0x1f0 dprc_get_obj_region+0xfc/0x1c0	N/A	More Details

	fsl_mc_device_add+0x340/0x590 fsl_mc_obj_device_add+0xd0/0xf8 dprc_scan_objects+0x1c4/0x340 dprc_scan_container+0x38/0x60 vfio_fsl_mc_probe+0x9c/0xf8 fsl_mc_driver_probe+0x24/0x70 really_probe+0xbc/0x2a8 __driver_probe_device+0x78/0xe0 device_driver_attach+0x30/0x68 bind_store+0xa8/0x130 drv_attr_store+0x24/0x38 sysfs_kf_write+0x44/0x60 kernfs_fop_write_iter+0x128/0x1b8 vfs_write+0x334/0x448 ksys_write+0x68/0xf0 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x44/0x108 el0_svc_common.constprop.1+0x94/0xf8 do_el0_svc+0x38/0xb0 el0_svc+0x20/0x50 el0t_64_sync_handler+0x98/0xc0 el0t_64_sync+0x174/0x178 Code: aa0103f4 a9025bf5 d5384100 b9400801 (79401260) ---[end trace 0000000000000000]---		
CVE-2023-53363	In the Linux kernel, the following vulnerability has been resolved: PCI: Fix use-after-free in pci_bus_release_domain_nr() Commit c14f7ccc9f5d ("PCI: Assign PCI domain IDs by ida_alloc()") introduced a use-after-free bug in the bus removal cleanup. The issue was found with kfence: [19.293351] BUG: KFENCE: use-after-free read in pci_bus_release_domain_nr+0x10/0x70 [19.302817] Use-after-free read at 0x000000007f3b80eb (in kfence-#115): [19.309677] pci_bus_release_domain_nr+0x10/0x70 [19.309691] dw_pcie_host_deinit+0x28/0x78 [19.309702] tegra_pcie_deinit_controller+0x1c/0x38 [pcie_tegra194] [19.309734] tegra_pcie_dw_probe+0x648/0xb28 [pcie_tegra194] [19.309752] platform_probe+0x90/0xd8 ... [19.311457] kfence-#115: 0x00000000063a155a-0x00000000ba698da8, size=1072, cache=kmalloc-2k [19.311469] allocated by task 96 on cpu 10 at 19.279323s: [19.311562] __kmem_cache_alloc_node+0x260/0x278 [19.311571] kmalloc_trace+0x24/0x30 [19.311580] pci_alloc_bus+0x24/0xa0 [19.311590] pci_register_host_bridge+0x48/0x4b8 [19.311601] pci_scan_root_bus_bridge+0xc0/0xe8 [19.311613] pci_host_probe+0x18/0xc0 [19.311623] dw_pcie_host_init+0x2c0/0x568 [19.311630] tegra_pcie_dw_probe+0x610/0xb28 [pcie_tegra194] [19.311647] platform_probe+0x90/0xd8 ... [19.311782] freed by task 96 on cpu 10 at 19.285833s: [19.311799] release_pcibus_dev+0x30/0x40 [19.311808] device_release+0x30/0x90 [19.311814] kobject_put+0xa8/0x120 [19.311832] device_unregister+0x20/0x30 [19.311839] pci_remove_bus+0x78/0x88 [19.311850] pci_remove_root_bus+0x5c/0x98 [19.311860] dw_pcie_host_deinit+0x28/0x78 [19.311866] tegra_pcie_deinit_controller+0x1c/0x38 [pcie_tegra194] [19.311883] tegra_pcie_dw_probe+0x648/0xb28 [pcie_tegra194] [19.311900] platform_probe+0x90/0xd8 ... [19.313579] CPU: 10 PID: 96 Comm: kworker/u24:2 Not tainted 6.2.0 #4 [19.320171] Hardware name: /, BIOS 1.0-d7fb19b 08/10/2022 [19.325852] Workqueue: events_unbound deferred_probe_work_func The stack trace is a bit misleading as dw_pcie_host_deinit() doesn't directly call pci_bus_release_domain_nr(). The issue turns out to be in pci_remove_root_bus() which first calls pci_remove_bus() which frees the struct pci_bus when its struct device is released. Then pci_bus_release_domain_nr() is called and accesses the freed struct pci_bus. Reordering these fixes the issue.	N/A	More Details
CVE-2025-43809	Cross-Site Request Forgery (CSRF) vulnerability in the server (license) registration page in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.7, 2023.Q3.1 through 2023.Q3.9, 7.4 GA through update 92, and older unsupported versions allows remote attackers to register a server license via the 'orderUuid' parameter.	N/A	More Details
CVE-2025-39842	In the Linux kernel, the following vulnerability has been resolved: ocfs2: prevent release journal inode after journal shutdown Before calling ocfs2_delete_osb(), ocfs2_journal_shutdown() has already been executed in ocfs2_dismount_volume(), so osb->journal must be NULL. Therefore, the following calltrace will inevitably fail when it reaches jbd2_journal_release_jbd_inode(). ocfs2_dismount_volume()-> ocfs2_delete_osb()-> ocfs2_free_slot_info()-> __ocfs2_free_slot_info()-> evict()-> ocfs2_evict_inode()-> ocfs2_clear_inode()-> jbd2_journal_release_jbd_inode(osb->journal->j_journal, Adding osb->journal checks will prevent null-ptr-deref during the above execution path.	N/A	More Details
CVE-2023-53364	In the Linux kernel, the following vulnerability has been resolved: regulator: da9063: better fix null deref with partial DT Two versions of the original patch were sent but V1 was merged instead of V2 due to a mistake. So update to V2. The advantage of V2 is that it completely avoids dereferencing the pointer, even just to take the address, which may fix problems with some compilers. Both versions work on my gcc 9.4 but use the safer one.	N/A	More Details
CVE-2023-53365	In the Linux kernel, the following vulnerability has been resolved: ip6mr: Fix skb_under_panic in ip6mr_cache_report() skbuff: skb_under_panic: text:ffffffff88771f69 len:56 put:-4 head:ffff88805f86a800 data:ffff887f5f86a850 tail:0x88 end:0x2c0 dev:pim6reg ------------[cut here]------------ kernel BUG at net/core/skbuff.c:192! invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 2 PID: 22968 Comm: kworker/2:11 Not tainted 6.5.0-rc3-00044-g0a8db05b571a #236 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: ipv6_addrconf addrconf_dad_work RIP: 0010:skb_panic+0x152/0x1d0 Call Trace: <TASK> skb_push+0xc4/0xe0 ip6mr_cache_report+0xd69/0x19b0 reg_vif_xmit+0x406/0x690 dev_hard_start_xmit+0x17e/0x6e0 __dev_queue_xmit+0x2d6a/0x3d20 vlan_dev_hard_start_xmit+0x3ab/0x5c0 dev_hard_start_xmit+0x17e/0x6e0 __dev_queue_xmit+0x2d6a/0x3d20 neigh_connected_output+0x3ed/0x570 ip6_finish_output2+0x5b5/0x1950 ip6_finish_output+0x693/0x11c0 ip6_output+0x24b/0x880 NF_HOOK.constprop.0+0xfd/0x530 ndisc_send_skb+0x9db/0x1400 ndisc_send_rs+0x12a/0x6c0 addrconf_dad_completed+0x3c9/0xea0 addrconf_dad_work+0x849/0x1420 process_one_work+0xa22/0x16e0 worker_thread+0x679/0x10c0 ret_from_fork+0x28/0x60 ret_from_fork_asm+0x11/0x20 When setup a vlan device on dev pim6reg, DAD ns packet may sent on reg_vif_xmit(). reg_vif_xmit() ip6mr_cache_report() skb_push(skb, -skb_network_offset(pkt));//skb_network_offset(pkt) is 4 And skb_push declared as: void *skb_push(struct	N/A	More Details

	sk_buff *skb, unsigned int len); skb->data -= len; //0xffff88805f86a84c - 0xffffffc = 0xffff887f5f86a850 skb->data is set to 0xffff887f5f86a850, which is invalid mem addr, lead to skb_push() fails.		
CVE-2023-53366	In the Linux kernel, the following vulnerability has been resolved: block: be a bit more careful in checking for NULL bdev while polling Wei reports a crash with an application using polled IO: PGD 14265e067 P4D 14265e067 PUD 47ec50067 PMD 0 Oops: 0000 [#1] SMP CPU: 0 PID: 21915 Comm: iocore_0 Kdump: loaded Tainted: G S 5.12.0-0_fbk12_clang_7346_g1bb6f2e7058f #1 Hardware name: Wiwynn Delta Lake MP T8/Delta Lake-Class2, BIOS Y3DLM08 04/10/2022 RIP: 0010:bio_poll+0x25/0x200 Code: 0f 1f 44 00 00 0f 1f 44 00 00 55 41 57 41 56 41 55 41 54 53 48 83 ec 28 65 48 8b 04 25 28 00 00 00 48 89 44 24 20 48 8b 47 08 <48> 8b 80 70 02 00 00 4c 8b 70 50 8b 6f 34 31 db 83 fd ff 75 25 65 RSP: 0018:ffffc90005fafdf8 EFLAGS: 00010292 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 74b43cd65dd66600 RDX: 0000000000000003 RSI: ffffc90005fafe78 RDI: ffff8884b614e140 RBP: ffff88849964df78 R08: 0000000000000000 R09: 0000000000000008 R10: 0000000000000000 R11: 0000000000000000 R12: ffff88849964df00 R13: ffffc90005fafe78 R14: ffff888137d3c378 R15: 0000000000000001 FS: 00007fd195000640(0000) GS:ffff88903f400000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000270 CR3: 0000000466121001 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: iocb_bio_iopoll+0x1d/0x30 io_do_iopoll+0xac/0x250 __se_sys_io_uring_enter+0x3c5/0x5a0 ? __x64_sys_write+0x89/0xd0 do_syscall_64+0x2d/0x40 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x94f225d Code: 24 cc 00 00 00 41 8b 84 24 d0 00 00 00 c1 e0 04 83 e0 10 41 09 c2 8b 33 8b 53 04 4c 8b 43 18 4c 63 4b 0c b8 aa 01 00 00 0f 05 <85> c0 0f 88 85 00 00 00 29 03 45 84 f6 0f 84 88 00 00 00 41 f6 c7 RSP: 002b:00007fd194ffcd88 EFLAGS: 00000202 ORIG_RAX: 00000000000001aa RAX: ffffffffffffffda RBX: 00007fd194ffcdc0 RCX: 00000000094f225d RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000007 RBP: 00007fd194ffcdb0 R08: 0000000000000000 R09: 0000000000000008 R10: 0000000000000001 R11: 0000000000000202 R12: 00007fd269d68030 R13: 0000000000000000 R14: 0000000000000001 R15: 0000000000000000 which is due to bio->bi_bdev being NULL. This can happen if we have two tasks doing polled IO, and task B ends up completing IO from task A if they are sharing a poll queue. If task B completes the IO and puts the bio into our cache, then it can allocate that bio again before task A is done polling for it. As that would necessitate a preempt between the two tasks, it's enough to just be a bit more careful in checking for whether or not bio->bi_bdev is NULL.	N/A	More Details
CVE-2025-39841	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix buffer free/clear order in deferred receive path Fix a use-after-free window by correcting the buffer release sequence in the deferred receive path. The code freed the RQ buffer first and only then cleared the context pointer under the lock. Concurrent paths (e.g., ABTS and the repost path) also inspect and release the same pointer under the lock, so the old order could lead to double-free/UAF. Note that the repost path already uses the correct pattern: detach the pointer under the lock, then free it after dropping the lock. The deferred path should do the same.	N/A	More Details
CVE-2023-53367	In the Linux kernel, the following vulnerability has been resolved: accel/habanalabs: fix mem leak in capture user mappings This commit fixes a memory leak caused when clearing the user_mappings info when a new context is opened immediately after user_mapping is captured and a hard reset is performed.	N/A	More Details
CVE-2023-53355	In the Linux kernel, the following vulnerability has been resolved: staging: pi433: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once. This requires saving off the root directory dentry to make creation of individual device subdirectories easier.	N/A	More Details
CVE-2023-53354	In the Linux kernel, the following vulnerability has been resolved: skbuff: skb_segment, Call zero copy functions before using skbuff frags Commit bf5c25d60861 ("skbuff: in skb_segment, call zerocopy functions once per nskb") added the call to zero copy functions in skb_segment(). The change introduced a bug in skb_segment() because skb_orphan_frags() may possibly change the number of fragments or allocate new fragments altogether leaving nrfrags and frag to point to the old values. This can cause a panic with stacktrace like the one below. [193.894380] BUG: kernel NULL pointer dereference, address: 00000000000000bc [193.895273] CPU: 13 PID: 18164 Comm: vh-net-17428 Kdump: loaded Tainted: G O 5.15.123+ #26 [193.903919] RIP: 0010:skb_segment+0xb0e/0x12f0 [194.021892] Call Trace: [194.027422] <TASK> [194.072861] tcp_gso_segment+0x107/0x540 [194.082031] inet_gso_segment+0x15c/0x3d0 [194.090783] skb_mac_gso_segment+0x9f/0x110 [194.095016] __skb_gso_segment+0xc1/0x190 [194.103131] netem_enqueue+0x290/0xb10 [sch_netem] [194.107071] dev_qdisc_enqueue+0x16/0x70 [194.110884] __dev_queue_xmit+0x63b/0xb30 [194.121670] bond_start_xmit+0x159/0x380 [bonding] [194.128506] dev_hard_start_xmit+0xc3/0x1e0 [194.131787] __dev_queue_xmit+0x8a0/0xb30 [194.138225] macvlan_start_xmit+0x4f/0x100 [macvlan] [194.141477] dev_hard_start_xmit+0xc3/0x1e0 [194.144622] sch_direct_xmit+0xe3/0x280 [194.147748] __dev_queue_xmit+0x54a/0xb30 [194.154131] tap_get_user+0x2a8/0x9c0 [tap] [194.157358] tap_sendmsg+0x52/0x8e0 [tap] [194.167049] handle_tx_zerocopy+0x14e/0x4c0 [vhost_net] [194.173631] handle_tx+0xcd/0xe0 [vhost_net] [194.176959] vhost_worker+0x76/0xb0 [vhost] [194.183667] kthread+0x118/0x140 [194.190358] ret_from_fork+0x1f/0x30 [194.193670] </TASK> In this case calling skb_orphan_frags() updated nr_frags leaving nrfrags local variable in skb_segment() stale. This resulted in the code hitting i >= nrfrags prematurely and trying to move to next frag_skb using list_skb pointer, which was NULL, and caused kernel panic. Move the call to zero copy functions before using frags and nr_frags.	N/A	More Details

CVE-2023-53353	In the Linux kernel, the following vulnerability has been resolved: accel/habanalabs: postpone mem_mgr IDR destruction to hpriv_release() The memory manager IDR is currently destroyed when user releases the file descriptor. However, at this point the user context might be still held, and memory buffers might be still in use. Later on, calls to release those buffers will fail due to not finding their handles in the IDR, leading to a memory leak. To avoid this leak, split the IDR destruction from the memory manager fini, and postpone it to hpriv_release() when there is no user context and no buffers are used.	N/A	More Details
CVE-2023-53344	In the Linux kernel, the following vulnerability has been resolved: can: bcm: bcm_tx_setup(): fix KMSAN uninit-value in vfs_write Syzkaller reported the following issue: === BUG: KMSAN: uninit-value in aio_rw_done fs/aio.c:1520 [inline] BUG: KMSAN: uninit-value in aio_write+0x899/0x950 fs/aio.c:1600 aio_rw_done fs/aio.c:1520 [inline] aio_write+0x899/0x950 fs/aio.c:1600 io_submit_one+0x1d1c/0x3bf0 fs/aio.c:2019 __do_sys_io_submit fs/aio.c:2078 [inline] __se_sys_io_submit+0x293/0x770 fs/aio.c:2048 __x64_sys_io_submit+0x92/0xd0 fs/aio.c:2048 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd Uninit was created at: slab_post_alloc_hook mm/slab.h:766 [inline] slab_alloc_node mm/slub.c:3452 [inline] __kmem_cache_alloc_node+0x71f/0xce0 mm/slub.c:3491 __do_kmalloc_node mm/slab_common.c:967 [inline] __kmalloc+0x11d/0x3b0 mm/slab_common.c:981 kmalloc_array include/linux/slab.h:636 [inline] bcm_tx_setup+0x80e/0x29d0 net/can/bcm.c:930 bcm_sendmsg+0x3a2/0xce0 net/can/bcm.c:1351 sock_sendmsg_nosec net/socket.c:714 [inline] sock_sendmsg net/socket.c:734 [inline] sock_write_iter+0x495/0x5e0 net/socket.c:1108 call_write_iter include/linux/fs.h:2189 [inline] aio_write+0x63a/0x950 fs/aio.c:1600 io_submit_one+0x1d1c/0x3bf0 fs/aio.c:2019 __do_sys_io_submit fs/aio.c:2078 [inline] __se_sys_io_submit+0x293/0x770 fs/aio.c:2048 __x64_sys_io_submit+0x92/0xd0 fs/aio.c:2048 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd CPU: 1 PID: 5034 Comm: syz-executor350 Not tainted 6.2.0-rc6-syzkaller-80422-geda666ff2276 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/12/2023 === We can follow the call chain and find that 'bcm_tx_setup' function calls 'memcpy_from_msg' to copy some content to the newly allocated frame of 'op->frames'. After that the 'len' field of copied structure being compared with some constant value (64 or 8). However, if 'memcpy_from_msg' returns an error, we will compare some uninitialized memory. This triggers 'uninit-value' issue. This patch will add 'memcpy_from_msg' possible errors processing to avoid uninit-value issue. Tested via syzkaller	N/A	More Details
CVE-2025-57203	MagicProject AI version 9.1 is affected by a Cross-Site Scripting (XSS) vulnerability within the chatbot generation feature available to authenticated admin users. The vulnerability resides in the prompt parameter submitted to the /dashboard/user/generator/generate-stream endpoint via a multipart/form-data POST request. Due to insufficient input sanitization, attackers can inject HTML-based JavaScript payloads. This payload is stored and rendered unsanitized in subsequent views, leading to execution in other users' browsers when they access affected content. This issue allows an authenticated attacker to execute arbitrary JavaScript in the context of another user, potentially leading to session hijacking, privilege escalation, data exfiltration, or administrative account takeover. The application does not implement a Content Security Policy (CSP) or adequate input filtering to prevent such attacks. A fix should include proper sanitization, output encoding, and strong CSP enforcement to mitigate exploitation.	N/A	More Details
CVE-2023-53338	In the Linux kernel, the following vulnerability has been resolved: lwt: Fix return values of BPF xmit ops BPF encap ops can return different types of positive values, such like NET_RX_DROP, NET_XMIT_CN, NETDEV_TX_BUSY, and so on, from function skb_do_redirect and bpf_lwt_xmit_reroute. At the xmit hook, such return values would be treated implicitly as LWTUNNEL_XMIT_CONTINUE in ip(6)_finish_output2. When this happens, skbs that have been freed would continue to the neighbor subsystem, causing use-after-free bug and kernel crashes. To fix the incorrect behavior, skb_do_redirect return values can be simply discarded, the same as tc-egress behavior. On the other hand, bpf_lwt_xmit_reroute returns useful errors to local senders, e.g. PMTU information. Thus convert its return values to avoid the conflict with LWTUNNEL_XMIT_CONTINUE.	N/A	More Details
CVE-2023-53339	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix BUG_ON condition in btrfs_cancel_balance Pausing and canceling balance can race to interrupt balance lead to BUG_ON panic in btrfs_cancel_balance. The BUG_ON condition in btrfs_cancel_balance does not take this race scenario into account. However, the race condition has no other side effects. We can fix that. Reproducing it with panic trace like this: kernel BUG at fs/btrfs/volumes.c:4618! RIP: 0010:btrfs_cancel_balance+0x5cf/0x6a0 Call Trace: <TASK> ? do_nanosleep+0x60/0x120 ? hrtimer_nanosleep+0xb7/0x1a0 ? sched_core_clone_cookie+0x70/0x70 btrfs_ioctl_balance_ctl+0x55/0x70 btrfs_ioctl+0xa46/0xd20 __x64_sys_ioctl+0x7d/0xa0 do_syscall_64+0x38/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd Race scenario as follows: > mutex_unlock(&fs_info->balance_mutex); > ---------- > .....issue pause and cancel req in another thread > ---------- > ret = __btrfs_balance(fs_info); > > mutex_lock(&fs_info->balance_mutex); > if (ret == -ECANCELED && atomic_read(&fs_info->balance_pause_req)) { > btrfs_info(fs_info, "balance: paused"); > btrfs_exclop_balance(fs_info, BTRFS_EXCLOP_BALANCE_PAUSED); > }	N/A	More Details
CVE-2025-	Rejected reason: Not used	N/A	More

59883			Details
CVE-2023-53340	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Collect command failures data only for known commands DEVX can issue a general command, which is not used by mlx5 driver. In case such command is failed, mlx5 is trying to collect the failure data, However, mlx5 doesn't create a storage for this command, since mlx5 doesn't use it. This lead to array-index-out-of-bounds error. Fix it by checking whether the command is known before collecting the failure data.	N/A	More Details
CVE-2023-53341	In the Linux kernel, the following vulnerability has been resolved: of/fdt: run soc memory setup when early_init_dt_scan_memory fails If memory has been found early_init_dt_scan_memory now returns 1. If it hasn't found any memory it will return 0, allowing other memory setup mechanisms to carry on. Previously early_init_dt_scan_memory always returned 0 without distinguishing between any kind of memory setup being done or not. Any code path after the early_init_dt_scan memory call in the ramips plat_mem_setup code wouldn't be executed anymore. Making early_init_dt_scan_memory the only way to initialize the memory. Some boards, including my mt7621 based Cudy X6 board, depend on memory initialization being done via the soc_info.mem_detect function pointer. Those wouldn't be able to obtain memory and panic the kernel during early bootup with the message "early_init_dt_alloc_memory_arch: Failed to allocate 12416 bytes align=0x40".	N/A	More Details
CVE-2025-34199	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 22.0.1049 and Application versions prior to 20.0.2786 (VA and SaaS deployments) contain insecure defaults and code patterns that disable TLS/SSL certificate verification for communications to printers and internal microservices. In multiple places, the application sets libcurl/PHP transport options such that CURLOPT_SSL_VERIFYHOST and CURLOPT_SSL_VERIFYPEER are effectively disabled, and environment variables (for example API_*_VERIFYSSL=false) are used to turn off verification for gateway and microservice endpoints. As a result, the client accepts TLS connections without validating server certificates (and, in some cases, uses clear-text HTTP), permitting on-path attackers to perform man-in-the-middle (MitM) attacks. An attacker able to intercept network traffic between the product and printers or microservices can eavesdrop on and modify sensitive data (including print jobs, configuration, and authentication tokens), inject malicious payloads, or disrupt service.	N/A	More Details
CVE-2023-53342	In the Linux kernel, the following vulnerability has been resolved: net: marvell: prestera: fix handling IPv4 routes with nhid Fix handling IPv4 routes referencing a nexthop via its id by replacing calls to fib_info_nh() with fib_info_nhc(). Trying to add an IPv4 route referencing a nextop via nhid: $ ip link set up swp5 $ ip a a 10.0.0.1/24 dev swp5 $ ip nexthop add dev swp5 id 20 via 10.0.0.2 $ ip route add 10.0.1.0/24 nhid 20 triggers warnings when trying to handle the route: [528.805763] ------------[cut here]------------ [528.810437] WARNING: CPU: 3 PID: 53 at include/net/nexthop.h:468 __prestera_fi_is_direct+0x2c/0x68 [prestera] [528.820434] Modules linked in: prestera_pci act_gact act_police sch_ingress cls_u32 cls_flower prestera arm64_delta_tn48m_dn_led(O) arm64_delta_tn48m_dn_cpld(O) [last unloaded: prestera_pci] [528.837485] CPU: 3 PID: 53 Comm: kworker/u8:3 Tainted: G O 6.4.5 #1 [528.845178] Hardware name: delta,tn48m-dn (DT) [528.849641] Workqueue: prestera_ordered __prestera_router_fib_event_work [prestera] [528.857352] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [528.864347] pc : __prestera_fi_is_direct+0x2c/0x68 [prestera] [528.870135] lr : prestera_k_arb_fib_evt+0xb20/0xd50 [prestera] [528.876007] sp : ffff80000b20bc90 [528.879336] x29: ffff80000b20bc90 x28: 0000000000000000 x27: ffff0001374d3a48 [528.886510] x26: ffff000105604000 x25: ffff000134af8a28 x24: ffff0001374d3800 [528.893683] x23: ffff000101c89148 x22: ffff000101c89000 x21: ffff000101c89200 [528.900855] x20: ffff00013641fda0 x19: ffff800009d01088 x18: 0000000000000059 [528.908027] x17: 0000000000000277 x16: 0000000000000000 x15: 0000000000000000 [528.915198] x14: 0000000000000003 x13: 00000000000fe400 x12: 0000000000000000 [528.922371] x11: 0000000000000002 x10: 0000000000000aa0 x9 : ffff8000013d2020 [528.929543] x8 : 0000000000000018 x7 : 000000007b1703f8 x6 : 000000001ca72f86 [528.936715] x5 : 0000000033399ea7 x4 : 0000000000000000 x3 : ffff0001374d3acc [528.943886] x2 : 0000000000000000 x1 : ffff00010200de00 x0 : ffff000134ae3f80 [528.951058] Call trace: [528.953516] __prestera_fi_is_direct+0x2c/0x68 [prestera] [528.958952] __prestera_router_fib_event_work+0x100/0x158 [prestera] [528.965348] process_one_work+0x208/0x488 [528.969387] worker_thread+0x4c/0x430 [528.973068] kthread+0x120/0x138 [528.976313] ret_from_fork+0x10/0x20 [528.979909] ---[end trace 0000000000000000]--- [528.984998] ------------[cut here]------------ [528.989645] WARNING: CPU: 3 PID: 53 at include/net/nexthop.h:468 __prestera_fi_is_direct+0x2c/0x68 [prestera] [528.999628] Modules linked in: prestera_pci act_gact act_police sch_ingress cls_u32 cls_flower prestera arm64_delta_tn48m_dn_led(O) arm64_delta_tn48m_dn_cpld(O) [last unloaded: prestera_pci] [529.016676] CPU: 3 PID: 53 Comm: kworker/u8:3 Tainted: G W O 6.4.5 #1 [529.024368] Hardware name: delta,tn48m-dn (DT) [529.028830] Workqueue: prestera_ordered __prestera_router_fib_event_work [prestera] [529.036539] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [529.043533] pc : __prestera_fi_is_direct+0x2c/0x68 [prestera] [529.049318] lr : __prestera_k_arb_fc_apply+0x280/0x2f8 [prestera] [529.055452] sp : ffff80000b20bc60 [529.058781] x29: ffff80000b20bc60 x28: 0000000000000000 x27: ffff0001374d3a48 [529.065953] x26: ffff000105604000 x25: ffff000134af8a28 x24: ffff0001374d3800 [529.073126] x23: ffff000101c89148 x22: ffff000101c89148 x21: ffff00013641fda0 [529.080299] x20: ffff000101c89000 x19: ffff000101c89020 x18: 0000000000000059 [529.087471] x17: 0000000000000277 x16: 0000000000000000 x15: 0000000000000000 [529.094642] x14: 0000000000000003 x13: 00000000000fe400 x12: 0000000000000000 [529.101814] x11: 0000000000000002 x10:	N/A	More Details

	0000000000000aa0 x9 : ffff8000013cee80 [529.108985] x8 : 0000000000000018 x7 : 000000007b1703f8 x6 ---truncated---		
CVE-2023-53343	In the Linux kernel, the following vulnerability has been resolved: icmp6: Fix null-ptr-deref of ip6_null_entry->rt6i_idev in icmp6_dev(). With some IPv6 Ext Hdr (RPL, SRv6, etc.), we can send a packet that has the link-local address as src and dst IP and will be forwarded to an external IP in the IPv6 Ext Hdr. For example, the script below generates a packet whose src IP is the link-local address and dst is updated to 11::. # for f in $(find /proc/sys/net/ -name *seg6_enabled*); do echo 1 > $f; done # python3 >>> from socket import * >>> from scapy.all import * >>> >>> SRC_ADDR = DST_ADDR = "fe80::5054:ff:fe12:3456" >>> >>> pkt = IPv6(src=SRC_ADDR, dst=DST_ADDR) >>> pkt /= IPv6ExtHdrSegmentRouting(type=4, addresses=["11::", "22::"], segleft=1) >>> >>> sk = socket(AF_INET6, SOCK_RAW, IPPROTO_RAW) >>> sk.sendto(bytes(pkt), (DST_ADDR, 0)) For such a packet, we call ip6_route_input() to look up a route for the next destination in these three functions depending on the header type. * ipv6_rthdr_rcv() * ipv6_rpl_srh_rcv() * ipv6_srh_rcv() If no route is found, ip6_null_entry is set to skb, and the following dst_input(skb) calls ip6_pkt_drop(). Finally, in icmp6_dev(), we dereference skb_rt6_info(skb)->rt6i_idev->dev as the input device is the loopback interface. Then, we have to check if skb_rt6_info(skb)->rt6i_idev is NULL or not to avoid NULL pointer deref for ip6_null_entry. BUG: kernel NULL pointer dereference, address: 0000000000000000 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 0 PID: 157 Comm: python3 Not tainted 6.4.0-11996-gb121d614371c #35 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:icmp6_send (net/ipv6/icmp.c:436 net/ipv6/icmp.c:503) Code: fe ff ff 48 c7 40 30 c0 86 5d 83 e8 c6 44 1c 00 e9 c8 fc ff ff 49 8b 46 58 48 83 e0 fe 0f 84 4a fb ff ff 48 8b 80 d0 00 00 00 <48> 8b 00 44 8b 88 e0 00 00 00 e9 34 fb ff ff 4d 85 ed 0f 85 69 01 RSP: 0018:ffffc90000003c70 EFLAGS: 00000286 RAX: 0000000000000000 RBX: 0000000000000001 RCX: 00000000000000e0 RDX: 0000000000000021 RSI: 0000000000000000 RDI: ffff888006d72a18 RBP: ffffc90000003d80 R08: 0000000000000000 R09: 0000000000000001 R10: ffffc90000003d98 R11: 0000000000000040 R12: ffff888006d72a10 R13: 0000000000000000 R14: ffff8880057fb800 R15: ffffffff835d86c0 FS: 00007f9dc72ee740(0000) GS:ffff88807dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000000057b2000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <IRQ> ip6_pkt_drop (net/ipv6/route.c:4513) ipv6_rthdr_rcv (net/ipv6/exthdrs.c:640 net/ipv6/exthdrs.c:686) ip6_protocol_deliver_rcu (net/ipv6/ip6_input.c:437 (discriminator 5)) ip6_input_finish (./include/linux/rcupdate.h:781 net/ipv6/ip6_input.c:483) __netif_receive_skb_one_core (net/core/dev.c:5455) process_backlog (./include/linux/rcupdate.h:781 net/core/dev.c:5895) __napi_poll (net/core/dev.c:6460) net_rx_action (net/core/dev.c:6529 net/core/dev.c:6660) __do_softirq (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:207 ./include/trace/events/irq.h:142 kernel/softirq.c:554) do_softirq (kernel/softirq.c:454 kernel/softirq.c:441) </IRQ> <TASK> __local_bh_enable_ip (kernel/softirq.c:381) __dev_queue_xmit (net/core/dev.c:4231) ip6_finish_output2 (./include/net/neighbour.h:544 net/ipv6/ip6_output.c:135) rawv6_sendmsg (./include/net/dst.h:458 ./include/linux/netfilter.h:303 net/ipv6/raw.c:656 net/ipv6/raw.c:914) sock_sendmsg (net/socket.c:725 net/socket.c:748) __sys_sendto (net/socket.c:2134) __x64_sys_sendto (net/socket.c:2146 net/socket.c:2142 net/socket.c:2142) do_syscall_64 (arch/x86/entry/common.c:50 arch/x86/entry/common.c:80) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:120) RIP: 0033:0x7f9dc751baea Code: d8 64 89 02 48 c7 c0 ff f ---truncated---	N/A	More Details
CVE-2023-53345	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix potential data race in rxrpc_wait_to_be_connected() Inside the loop in rxrpc_wait_to_be_connected() it checks call->error to see if it should exit the loop without first checking the call state. This is probably safe as if call->error is set, the call is dead anyway, but we should probably wait for the call state to have been set to completion first, lest it cause surprise on the way out. Fix this by only accessing call->error if the call is complete. We don't actually need to access the error inside the loop as we'll do that after. This caused the following report: BUG: KCSAN: data-race in rxrpc_send_data / rxrpc_set_call_completion write to 0xffff888159cf3c50 of 4 bytes by task 25673 on cpu 1: rxrpc_set_call_completion+0x71/0x1c0 net/rxrpc/call_state.c:22 rxrpc_send_data_packet+0xba9/0x1650 net/rxrpc/output.c:479 rxrpc_transmit_one+0x1e/0x130 net/rxrpc/output.c:714 rxrpc_decant_prepared_tx net/rxrpc/call_event.c:326 [inline] rxrpc_transmit_some_data+0x496/0x600 net/rxrpc/call_event.c:350 rxrpc_input_call_event+0x564/0x1220 net/rxrpc/call_event.c:464 rxrpc_io_thread+0x307/0x1d80 net/rxrpc/io_thread.c:461 kthread+0x1ac/0x1e0 kernel/kthread.c:376 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:308 read to 0xffff888159cf3c50 of 4 bytes by task 25672 on cpu 0: rxrpc_send_data+0x29e/0x1950 net/rxrpc/sendmsg.c:296 rxrpc_do_sendmsg+0xb7a/0xc20 net/rxrpc/sendmsg.c:726 rxrpc_sendmsg+0x413/0x520 net/rxrpc/af_rxrpc.c:565 sock_sendmsg_nosec net/socket.c:724 [inline] sock_sendmsg net/socket.c:747 [inline] ____sys_sendmsg+0x375/0x4c0 net/socket.c:2501 ___sys_sendmsg net/socket.c:2555 [inline] __sys_sendmmsg+0x263/0x500 net/socket.c:2641 __do_sys_sendmmsg net/socket.c:2670 [inline] __se_sys_sendmmsg net/socket.c:2667 [inline] __x64_sys_sendmmsg+0x57/0x60 net/socket.c:2667 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd value changed: 0x00000000 -> 0xfffffffea	N/A	More Details
CVE-2025-34202	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to 25.2.169 and Application prior to 25.2.1518 (VA and SaaS deployments) expose Docker internal networks in a way that allows an attacker on the same external L2 segment — or an attacker able to add routes using the appliance as a gateway — to reach container IPs directly. This grants access to internal services (HTTP APIs, Redis, MySQL, etc.) that are intended to be isolated inside the container network. Many of those services are accessible without	N/A	More Details

	authentication or are vulnerable to known exploitation chains. As a result, compromise of a single reachable endpoint or basic network access can enable lateral movement, remote code execution, data exfiltration, and full system compromise.		
CVE-2023-53346	In the Linux kernel, the following vulnerability has been resolved: kernel/fail_function: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53347	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Handle pairing of E-switch via uplink un/load APIs In case user switch a device from switchdev mode to legacy mode, mlx5 first unpair the E-switch and afterwards unload the uplink vport. From the other hand, in case user remove or reload a device, mlx5 first unload the uplink vport and afterwards unpair the E-switch. The latter is causing a bug[1], hence, handle pairing of E-switch as part of uplink un/load APIs. [1] In case VF_LAG is used, every tc fdb flow is duplicated to the peer esw. However, the original esw keeps a pointer to this duplicated flow, not the peer esw. e.g.: if user create tc fdb flow over esw0, the flow is duplicated over esw1, in FW/HW, but in SW, esw0 keeps a pointer to the duplicated flow. During module unload while a peer tc fdb flow is still offloaded, in case the first device to be removed is the peer device (esw1 in the example above), the peer net-dev is destroyed, and so the mlx5e_priv is memset to 0. Afterwards, the peer device is trying to unpair himself from the original device (esw0 in the example above). Unpair API invoke the original device to clear peer flow from its eswitch (esw0), but the peer flow, which is stored over the original eswitch (esw0), is trying to use the peer mlx5e_priv, which is memset to 0 and result in bellow kernel-oops. [157.964081] BUG: unable to handle page fault for address: 000000000002ce60 [157.964662] #PF: supervisor read access in kernel mode [157.965123] #PF: error_code(0x0000) - not-present page [157.965582] PGD 0 P4D 0 [157.965866] Oops: 0000 [#1] SMP [157.967670] RIP: 0010:mlx5e_tc_del_fdb_flow+0x48/0x460 [mlx5_core] [157.976164] Call Trace: [157.976437] <TASK> [157.976690] __mlx5e_tc_del_fdb_peer_flow+0xe6/0x100 [mlx5_core] [157.977230] mlx5e_tc_clean_fdb_peer_flows+0x67/0x90 [mlx5_core] [157.977767] mlx5_esw_offloads_unpair+0x2d/0x1e0 [mlx5_core] [157.984653] mlx5_esw_offloads_devcom_event+0xbf/0x130 [mlx5_core] [157.985212] mlx5_devcom_send_event+0xa3/0xb0 [mlx5_core] [157.985714] esw_offloads_disable+0x5a/0x110 [mlx5_core] [157.986209] mlx5_eswitch_disable_locked+0x152/0x170 [mlx5_core] [157.986757] mlx5_eswitch_disable+0x51/0x80 [mlx5_core] [157.987248] mlx5_unload+0x2a/0xb0 [mlx5_core] [157.987678] mlx5_uninit_one+0x5f/0xd0 [mlx5_core] [157.988127] remove_one+0x64/0xe0 [mlx5_core] [157.988549] pci_device_remove+0x31/0xa0 [157.988933] device_release_driver_internal+0x18f/0x1f0 [157.989402] driver_detach+0x3f/0x80 [157.989754] bus_remove_driver+0x70/0xf0 [157.990129] pci_unregister_driver+0x34/0x90 [157.990537] mlx5_cleanup+0xc/0x1c [mlx5_core] [157.990972] __x64_sys_delete_module+0x15a/0x250 [157.991398] ? exit_to_user_mode_prepare+0xea/0x110 [157.991840] do_syscall_64+0x3d/0x90 [157.992198] entry_SYSCALL_64_after_hwframe+0x46/0xb0	N/A	More Details
CVE-2023-53348	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix deadlock when aborting transaction during relocation with scrub Before relocating a block group we pause scrub, then do the relocation and then unpause scrub. The relocation process requires starting and committing a transaction, and if we have a failure in the critical section of the transaction commit path (transaction state >= TRANS_STATE_COMMIT_START), we will deadlock if there is a paused scrub. That results in stack traces like the following: [42.479] BTRFS info (device sdc): relocating block group 53876686848 flags metadata|raid6 [42.936] BTRFS warning (device sdc): Skipping commit of aborted transaction. [42.936] ------------[cut here]------------ [42.936] BTRFS: Transaction aborted (error -28) [42.936] WARNING: CPU: 11 PID: 346822 at fs/btrfs/transaction.c:1977 btrfs_commit_transaction+0xcc8/0xeb0 [btrfs] [42.936] Modules linked in: dm_flakey dm_mod loop btrfs (...) [42.936] CPU: 11 PID: 346822 Comm: btrfs Tainted: G W 6.3.0-rc2-btrfs-next-127+ #1 [42.936] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 [42.936] RIP: 0010:btrfs_commit_transaction+0xcc8/0xeb0 [btrfs] [42.936] Code: ff ff 45 8b (...) [42.936] RSP: 0018:ffffb58649633b48 EFLAGS: 00010282 [42.936] RAX: 0000000000000000 RBX: ffff8be6ef4d5bd8 RCX: 0000000000000000 [42.936] RDX: 0000000000000002 RSI: ffffffffb35e7782 RDI: 00000000ffffffff [42.936] RBP: ffff8be6ef4d5c98 R08: 0000000000000000 R09: ffffb586496339e8 [42.936] R10: 0000000000000001 R11: 0000000000000001 R12: ffff8be6d38c7c00 [42.936] R13: 00000000ffffffe4 R14: ffff8be6c268c000 R15: ffff8be6ef4d5cf0 [42.936] FS: 00007f381a82b340(0000) GS:ffff8beddfcc0000(0000) knlGS:0000000000000000 [42.936] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [42.936] CR2: 00007f1e35fb7638 CR3: 0000000117680006 CR4: 0000000000370ee0 [42.936] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [42.936] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [42.936] Call Trace: [42.936] <TASK> [42.936] ? start_transaction+0xcb/0x610 [btrfs] [42.936] prepare_to_relocate+0x111/0x1a0 [btrfs] [42.936] relocate_block_group+0x57/0x5d0 [btrfs] [42.936] ? btrfs_wait_nocow_writers+0x25/0xb0 [btrfs] [42.936] btrfs_relocate_block_group+0x248/0x3c0 [btrfs] [42.936] ? __pfx_autoremove_wake_function+0x10/0x10 [42.936] btrfs_relocate_chunk+0x3b/0x150 [btrfs] [42.936] btrfs_balance+0x8ff/0x11d0 [btrfs] [42.936] ? __kmem_cache_alloc_node+0x14a/0x410 [42.936] btrfs_ioctl+0x2334/0x32c0 [btrfs] [42.937] ? mod_objcg_state+0xd2/0x360 [42.937] ? refill_obj_stock+0xb0/0x160 [42.937] ? seq_release+0x25/0x30 [42.937] ? __rseq_handle_notify_resume+0x3b5/0x4b0 [42.937] ? percpu_counter_add_batch+0x2e/0xa0 [42.937] ? __x64_sys_ioctl+0x88/0xc0 [42.937] __x64_sys_ioctl+0x88/0xc0 [42.937] do_syscall_64+0x38/0x90 [42.937] entry_SYSCALL_64_after_hwframe+0x72/0xdc [42.937] RIP: 0033:0x7f381a6ffe9b [42.937] Code: 00 48 89 44 24 (...) [42.937] RSP: 002b:00007ffd45ecf060 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [42.937]	N/A	More Details

	RAX: ffffffffffffffda RBX: 0000000000000001 RCX: 00007f381a6ffe9b [42.937] RDX: 00007ffd45ecf150 RSI: 00000000c4009420 RDI: 0000000000000003 [42.937] RBP: 0000000000000003 R08: 0000000000000013 R09: 0000000000000000 [42.937] R10: 00007f381a60c878 R11: 0000000000000246 R12: 00007ffd45ed0423 [42.937] R13: 00007ffd45ecf150 R14: 0000000000000000 R15: 00007ffd45ecf148 [42.937] </TASK> [42.937] ---[end trace 0000000000000000]--- [42.937] BTRFS: error (device sdc: state A) in cleanup_transaction:1977: errno=-28 No space left [59.196] INFO: task btrfs:346772 blocked for more than 120 seconds. [59.196] Tainted: G W 6.3.0-rc2-btrfs-next-127+ #1 [59.196] "echo 0 > /proc/sys/kernel/hung_ ---truncated---		
CVE-2023-53349	In the Linux kernel, the following vulnerability has been resolved: media: ov2740: Fix memleak in ov2740_init_controls() There is a kmemleak when testing the media/i2c/ov2740.c with bpf mock device: unreferenced object 0xffff8881090e19e0 (size 16): comm "51-i2c-ov2740", pid 278, jiffies 4294781584 (age 23.613s) hex dump (first 16 bytes): 00 f3 7c 0b 81 88 ff ff 80 75 6a 09 81 88 ff ff ..|.....uj..... backtrace: [<000000004e9fad8f>] __kmalloc_node+0x44/0x1b0 [<0000000039c802f4>] kvmalloc_node+0x34/0x180 [<000000009b8b5c63>] v4l2_ctrl_handler_init_class+0x11d/0x180 [videodev] [<0000000038644056>] ov2740_probe+0x37d/0x84f [ov2740] [<0000000092489f59>] i2c_device_probe+0x28d/0x680 [<000000001038babe>] really_probe+0x17c/0x3f0 [<0000000098c7af1c>] __driver_probe_device+0xe3/0x170 [<00000000e1b3dc24>] device_driver_attach+0x34/0x80 [<000000005a04a34d>] bind_store+0x10b/0x1a0 [<00000000ce25d4f2>] drv_attr_store+0x49/0x70 [<000000007d9f4e9a>] sysfs_kf_write+0x8c/0xb0 [<00000000be6cff0f>] kernfs_fop_write_iter+0x216/0x2e0 [<0000000031ddb40a>] vfs_write+0x658/0x810 [<0000000041beecdd>] ksys_write+0xd6/0x1b0 [<0000000023755840>] do_syscall_64+0x38/0x90 [<00000000b2cc2da2>] entry_SYSCALL_64_after_hwframe+0x63/0xcd ov2740_init_controls() won't clean all the allocated resources in fail path, which may causes the memleaks. Add v4l2_ctrl_handler_free() to prevent memleak.	N/A	More Details
CVE-2025-34200	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (VA and SaaS deployments) provision the appliance with the network account credentials in clear-text inside /etc/issue, and the file is world-readable by default. An attacker with local shell access can read /etc/issue to obtain the network account username and password. Using the network account an attacker can change network parameters via the appliance interface, enabling local misconfiguration, network disruption or further escalation depending on deployment.	N/A	More Details
CVE-2023-53350	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Fix slicing memory leak The temporary buffer storing slicing configuration data from user is only freed on error. This is a memory leak. Free the buffer unconditionally.	N/A	More Details
CVE-2025-34201	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (VA and SaaS deployments) run many Docker containers on shared internal networks without firewalling or segmentation between instances. A compromise of any single container allows direct access to internal services (HTTP, Redis, MySQL, etc.) on the overlay network. From a compromised container, an attacker can reach and exploit other services, enabling lateral movement, data theft, and system-wide compromise.	N/A	More Details
CVE-2023-53351	In the Linux kernel, the following vulnerability has been resolved: drm/sched: Check scheduler work queue before calling timeout handling During an IGT GPU reset test we see again oops despite of commit 0c8c901aaaebc9 (drm/sched: Check scheduler ready before calling timeout handling). It uses ready condition whether to call drm_sched_fault which unwind the TDR leads to GPU reset. However it looks the ready condition is overloaded with other meanings, for example, for the following stack is related GPU reset : 0 gfx_v9_0_cp_gfx_start 1 gfx_v9_0_cp_gfx_resume 2 gfx_v9_0_cp_resume 3 gfx_v9_0_hw_init 4 gfx_v9_0_resume 5 amdgpu_device_ip_resume_phase2 does the following: /* start the ring */ gfx_v9_0_cp_gfx_start(adev); ring->sched.ready = true; The same approach is for other ASICs as well : gfx_v8_0_cp_gfx_resume gfx_v10_0_kiq_resume, etc... As a result, our GPU reset test causes GPU fault which calls unconditionally gfx_v9_0_fault and then drm_sched_fault. However now it depends on whether the interrupt service routine drm_sched_fault is executed after gfx_v9_0_cp_gfx_start is completed which sets the ready field of the scheduler to true even for uninitialized schedulers and causes oops vs no fault or when ISR drm_sched_fault is completed prior gfx_v9_0_cp_gfx_start and NULL pointer dereference does not occur. Use the field timeout_wq to prevent oops for uninitialized schedulers. The field could be initialized by the work queue of resetting the domain. v1: Corrections to commit message (Luben)	N/A	More Details
CVE-2023-53352	In the Linux kernel, the following vulnerability has been resolved: drm/ttm: check null pointer before accessing when swapping Add a check to avoid null pointer dereference as below: [90.002283] general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] PREEMPT SMP KASAN NOPTI [90.002292] KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] [90.002346] ? exc_general_protection+0x159/0x240 [90.002352] ? asm_exc_general_protection+0x26/0x30 [90.002357] ? ttm_bo_evict_swapout_allowable+0x322/0x5e0 [ttm] [90.002365] ? ttm_bo_evict_swapout_allowable+0x42e/0x5e0 [ttm] [90.002373] ttm_bo_swapout+0x134/0x7f0 [ttm] [90.002383] ? __pfx_ttm_bo_swapout+0x10/0x10 [ttm] [90.002391] ? lock_acquire+0x44d/0x4f0 [90.002398] ? ttm_device_swapout+0xa5/0x260 [ttm] [90.002412] ? lock_acquired+0x355/0xa00 [90.002416] ? do_raw_spin_trylock+0xb6/0x190 [90.002421] ? __pfx_lock_acquired+0x10/0x10 [90.002426] ? ttm_global_swapout+0x25/0x210 [ttm] [90.002442] ttm_device_swapout+0x198/0x260 [ttm] [90.002456] ? __pfx_ttm_device_swapout+0x10/0x10 [ttm] [90.002472] ttm_global_swapout+0x75/0x210 [ttm] [	N/A	More Details

	90.002486] ttm_tt_populate+0x187/0x3f0 [ttm] [90.002501] ttm_bo_handle_move_mem+0x437/0x590 [ttm] [90.002517] ttm_bo_validate+0x275/0x430 [ttm] [90.002530] ? __pfx_ttm_bo_validate+0x10/0x10 [ttm] [90.002544] ? kasan_save_stack+0x33/0x60 [90.002550] ? kasan_set_track+0x25/0x30 [90.002554] ? __kasan_kmalloc+0x8f/0xa0 [90.002558] ? amdgpu_gtt_mgr_new+0x81/0x420 [amdgpu] [90.003023] ? ttm_resource_alloc+0xf6/0x220 [ttm] [90.003038] amdgpu_bo_pin_restricted+0x2dd/0x8b0 [amdgpu] [90.003210] ? __x64_sys_ioctl+0x131/0x1a0 [90.003210] ? do_syscall_64+0x60/0x90		
CVE-2025-59882	Rejected reason: Not used	N/A	More Details
CVE-2022-50360	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dp: fix aux-bus EP lifetime Device-managed resources allocated post component bind must be tied to the lifetime of the aggregate DRM device or they will not necessarily be released when binding of the aggregate device is deferred. This can lead resource leaks or failure to bind the aggregate device when binding is later retried and a second attempt to allocate the resources is made. For the DP aux-bus, an attempt to populate the bus a second time will simply fail ("DP AUX EP device already populated"). Fix this by tying the lifetime of the EP device to the DRM device rather than DP controller platform device. Patchwork: https://patchwork.freedesktop.org/patch/502672/	N/A	More Details
CVE-2025-59884	Rejected reason: Not used	N/A	More Details
CVE-2025-1255	Untrusted Pointer Dereference vulnerability in RTI Connext Professional (Core Libraries) allows Pointer Manipulation.This issue affects Connext Professional: from 7.4.0 before 7.6.0, from 7.2.0 before 7.3.0.9.	N/A	More Details
CVE-2025-39860	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix use-after-free in l2cap_sock_cleanup_listen() syzbot reported the splat below without a repro. In the splat, a single thread calling bt_accept_dequeue() freed sk and touched it after that. The root cause would be the racy l2cap_sock_cleanup_listen() call added by the cited commit. bt_accept_dequeue() is called under lock_sock() except for l2cap_sock_release(). Two threads could see the same socket during the list iteration in bt_accept_dequeue(): CPU1 CPU2 (close()) ---- ---- sock_hold(sk) sock_hold(sk); lock_sock(sk) <-- block close() sock_put(sk) bt_accept_unlink(sk) sock_put(sk) <-- refcnt by bt_accept_enqueue() release_sock(sk) lock_sock(sk) sock_put(sk) bt_accept_unlink(sk) sock_put(sk) <-- last refcnt bt_accept_unlink(sk) <-- UAF Depending on the timing, the other thread could show up in the "Freed by task" part. Let's call l2cap_sock_cleanup_listen() under lock_sock() in l2cap_sock_release(). [0]: BUG: KASAN: slab-use-after-free in debug_spin_lock_before kernel/locking/spinlock_debug.c:86 [inline] BUG: KASAN: slab-use-after-free in do_raw_spin_lock+0x26f/0x2b0 kernel/locking/spinlock_debug.c:115 Read of size 4 at addr ffff88803b7eb1c4 by task syz.5.3276/16995 CPU: 3 UID: 0 PID: 16995 Comm: syz.5.3276 Not tainted syzkaller #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 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 mm/kasan/report.c:482 kasan_report+0xe0/0x110 mm/kasan/report.c:595 debug_spin_lock_before kernel/locking/spinlock_debug.c:86 [inline] do_raw_spin_lock+0x26f/0x2b0 kernel/locking/spinlock_debug.c:115 spin_lock_bh include/linux/spinlock.h:356 [inline] release_sock+0x21/0x220 net/core/sock.c:3746 bt_accept_dequeue+0x505/0x600 net/bluetooth/af_bluetooth.c:312 l2cap_sock_cleanup_listen+0x5c/0x2a0 net/bluetooth/l2cap_sock.c:1451 l2cap_sock_release+0x5c/0x210 net/bluetooth/l2cap_sock.c:1425 __sock_release+0xb3/0x270 net/socket.c:649 sock_close+0x1c/0x30 net/socket.c:1439 __fput+0x3ff/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+0x3f6/0x4c0 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f2accf8ebe9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffdb6cb1378 EFLAGS: 00000246 ORIG_RAX: 00000000000001b4 RAX: 0000000000000000 RBX: 00000000000426fb RCX: 00007f2accf8ebe9 RDX: 0000000000000000 RSI: 000000000000001e RDI: 0000000000000003 RBP: 00007f2acd1b7da0 R08: 0000000000000001 R09: 00000012b6cb166f R10: 0000001b30e20000 R11: 0000000000000246 R12: 00007f2acd1b609c R13: 00007f2acd1b6090 R14: ffffffffffffffff R15: 00007ffdb6cb1490 </TASK> Allocated by task 5326: kasan_save_stack+0x33/0x60 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:388 [inline] __kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:405 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4365 [inline] __kmalloc_nopro ---truncated---	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: vhci: Prevent use-after-free by removing debugfs files early Move the creation of debugfs files into a dedicated function, and ensure they are explicitly removed during vhci_release(), before associated data structures are freed. Previously, debugfs		

2025-39861	files such as "force_suspend", "force_wakeup", and others were created under hdev->debugfs but not removed in vhci_release(). Since vhci_release() frees the backing vhci_data structure, any access to these files after release would result in use-after-free errors. Although hdev->debugfs is later freed in hci_release_dev(), user can access files after vhci_data is freed but before hdev->debugfs is released.	N/A	More Details
CVE-2025-57639	OS Command injection vulnerability in Tenda AC9 1.0 was discovered to contain a command injection vulnerability via the usb.samba.guest.user parameter in the formSetSambaConf function of the httpd file.	N/A	More Details
CVE-2025-56394	Free5gc 4.0.1 is vulnerable to Buffer Overflow. The AMF incorrectly validates the 5GS mobile identity, resulting in slice reference overflow.	N/A	More Details
CVE-2025-55780	A null pointer dereference occurs in the function break_word_for_overflow_wrap() in MuPDF 1.26.4 when rendering a malformed EPUB document. Specifically, the function calls fz_html_split_flow() to split a FLOW_WORD node, but does not check if node->next is valid before accessing node->next->overflow_wrap, resulting in a crash if the split fails or returns a partial node chain.	N/A	More Details
CVE-2025-52905	Improper Input Validation vulnerability in TOTOLINK X6000R allows Flooding.This issue affects X6000R: through V9.4.0cu.1360_B20241207.	N/A	More Details
CVE-2025-4993	Untrusted Pointer Dereference vulnerability in RTI Connext Professional (Core Libraries) allows Pointer Manipulation.This issue affects Connext Professional: from 7.4.0 before 7.6.0, from 7.0.0 before 7.3.0.10, from 6.1.0 before 6.1.2.27, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*, from 4.4a before 5.2.*.	N/A	More Details
CVE-2025-4582	Buffer Over-read, Off-by-one Error vulnerability in RTI Connext Professional (Core Libraries) allows File Manipulation.This issue affects Connext Professional: from 7.4.0 before 7.6.0, from 7.0.0 before 7.3.0.8, from 6.1.0 before 6.1.2.26, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*, from 4.4a before 5.2.*.	N/A	More Details
CVE-2025-29084	SQL Injection vulnerability in CSZ-CMS v.1.3.0 allows a remote attacker to execute arbitrary code via the execSqlFile function in the Upgrade.php file.	N/A	More Details
CVE-2025-29083	SQL Injection vulnerability in CSZ-CMS v.1.3.0 allows a remote attacker to execute arbitrary code via the execSqlFile function in the Plugin_Manager.php file.	N/A	More Details
CVE-2025-39862	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7915: fix list corruption after hardware restart Since stations are recreated from scratch, all lists that wcids are added to must be cleared before calling ieee80211_restart_hw. Set wcid->sta = 0 for each wcid entry in order to ensure that they are not added again before they are ready.	N/A	More Details
CVE-2025-59548	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, specially crafted URLs to the FileBrowser are vulnerable to javascript injection, affecting any unsuspecting user clicking such link. This issue has been patched in version 10.1.0.	N/A	More Details
CVE-2025-39863	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: fix use-after-free when rescheduling brcmf_btcoex_info work The brcmf_btcoex_detach() only shuts down the btcoex timer, if the flag timer_on is false. However, the brcmf_btcoex_timerfunc(), which runs as timer handler, sets timer_on to false. This creates critical race conditions: 1.If brcmf_btcoex_detach() is called while brcmf_btcoex_timerfunc() is executing, it may observe timer_on as false and skip the call to timer_shutdown_sync(). 2.The brcmf_btcoex_timerfunc() may then reschedule the brcmf_btcoex_info worker after the cancel_work_sync() has been executed, resulting in use-after-free bugs. The use-after-free bugs occur in two distinct scenarios, depending on the timing of when the brcmf_btcoex_info struct is freed relative to the execution of its worker thread. Scenario 1: Freed before the worker is scheduled The brcmf_btcoex_info is deallocated before the worker is scheduled. A race condition can occur when schedule_work(&bt_local->work) is called after the target memory has been freed. The sequence of events is detailed below: CPU0 | CPU1 brcmf_btcoex_detach | brcmf_btcoex_timerfunc | bt_local->timer_on = false; if (cfg->btcoex->timer_on) | ... | cancel_work_sync(); | ... | kfree(cfg->btcoex); // FREE | | schedule_work(&bt_local->work); // USE Scenario 2: Freed after the worker is scheduled The brcmf_btcoex_info is freed after the worker has been scheduled but before or during its execution. In this case, statements within the brcmf_btcoex_handler() — such as the container_of macro and subsequent dereferences of the brcmf_btcoex_info object will cause a use-after-free access. The following timeline illustrates this scenario: CPU0 | CPU1 brcmf_btcoex_detach | brcmf_btcoex_timerfunc | bt_local->timer_on = false; if (cfg->btcoex->timer_on) | ... | cancel_work_sync(); | ... | schedule_work(); // Reschedule | kfree(cfg->btcoex); // FREE | brcmf_btcoex_handler() // Worker /* | btci = container_of(....); // USE The kfree() above could | ... also occur at any point | btci-> // USE during the worker's execution| */ | To resolve the race conditions, drop the conditional check and call timer_shutdown_sync() directly. It can deactivate the timer reliably, regardless of its current state. Once stopped, the timer_on state is then set to false.	N/A	More Details
CVE-2025-	Cross-site scripting (XSS) vulnerability in YzmCMS thru 7.3 via the referer header in the register page.	N/A	More Details

56304			
CVE-2025-39864	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: fix use-after-free in cmp_bss() Following bss_free() quirk introduced in commit 776b3580178f ("cfg80211: track hidden SSID networks properly"), adjust cfg80211_update_known_bss() to free the last beacon frame elements only if they're not shared via the corresponding 'hidden_beacon_bss' pointer.	N/A	More Details
CVE-2025-39865	In the Linux kernel, the following vulnerability has been resolved: tee: fix NULL pointer dereference in tee_shm_put tee_shm_put have NULL pointer dereference: __optee_disable_shm_cache --> shm = reg_pair_to_ptr(...);//shm maybe return NULL tee_shm_free(shm); --> tee_shm_put(shm);//crash Add check in tee_shm_put to fix it. panic log: Unable to handle kernel paging request at virtual address 0000000000100cca Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=0000002049d07000 [0000000000100cca] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP CPU: 2 PID: 14442 Comm: systemd-sleep Tainted: P OE ------- ---- 6.6.0-39-generic #38 Source Version: 938b255f6cb8817c95b0dd5c8c2944acfce94b07 Hardware name: greatwall GW-001Y1A-FTH, BIOS Great Wall BIOS V3.0 10/26/2022 pstate: 80000005 (Nzcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : tee_shm_put+0x24/0x188 lr : tee_shm_free+0x14/0x28 sp : ffff001f98f9faf0 x29: ffff001f98f9faf0 x28: ffff0020df543cc0 x27: 0000000000000000 x26: ffff001f811344a0 x25: ffff8000818dac00 x24: ffff800082d8d048 x23: ffff001f850fcd18 x22: 0000000000000001 x21: ffff001f98f9fb88 x20: ffff001f83e76218 x19: ffff001f83e761e0 x18: 000000000000ffff x17: 303a30303a303030 x16: 0000000000000000 x15: 0000000000000003 x14: 0000000000000001 x13: 0000000000000000 x12: 0101010101010101 x11: 0000000000000001 x10: 0000000000000001 x9 : ffff800080e08d0c x8 : ffff001f98f9fb88 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 x2 : ffff001f83e761e0 x1 : 00000000ffff001f x0 : 0000000000100cca Call trace: tee_shm_put+0x24/0x188 tee_shm_free+0x14/0x28 __optee_disable_shm_cache+0xa8/0x108 optee_shutdown+0x28/0x38 platform_shutdown+0x28/0x40 device_shutdown+0x144/0x2b0 kernel_power_off+0x3c/0x80 hibernate+0x35c/0x388 state_store+0x64/0x80 kobj_attr_store+0x14/0x28 sysfs_kf_write+0x48/0x60 kernfs_fop_write_iter+0x128/0x1c0 vfs_write+0x270/0x370 ksys_write+0x6c/0x100 __arm64_sys_write+0x20/0x30 invoke_syscall+0x4c/0x120 el0_svc_common.constprop.0+0x44/0xf0 do_el0_svc+0x24/0x38 el0_svc+0x24/0x88 el0t_64_sync_handler+0x134/0x150 el0t_64_sync+0x14c/0x15	N/A	More Details
CVE-2025-10155	An Improper Input Validation vulnerability in the scanning logic of mmaitre314 picklescan versions up to and including 0.0.30 allows a remote attacker to bypass pickle files security checks by supplying a standard pickle file with a PyTorch-related file extension. When the pickle file incorrectly considered safe is loaded, it can lead to the execution of malicious code.	N/A	More Details
CVE-2025-57407	A stored cross-site scripting (XSS) vulnerability in the Admin Log Viewer of S-Cart <=10.0.3 allows a remote authenticated attacker to inject arbitrary web script or HTML via a crafted User-Agent header. The script is executed in an administrator's browser when they view the security log page, which could lead to session hijacking or other malicious actions.	N/A	More Details
CVE-2025-39866	In the Linux kernel, the following vulnerability has been resolved: fs: writeback: fix use-after-free in __mark_inode_dirty() An use-after-free issue occurred when __mark_inode_dirty() get the bdi_writeback that was in the progress of switching. CPU: 1 PID: 562 Comm: systemd-random- Not tainted 6.6.56-gb4403bd46a8e #1 ..... pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __mark_inode_dirty+0x124/0x418 lr : __mark_inode_dirty+0x118/0x418 sp : ffffffc08c9dbbc0 ..... Call trace: __mark_inode_dirty+0x124/0x418 generic_update_time+0x4c/0x60 file_modified+0xcc/0xd0 ext4_buffered_write_iter+0x58/0x124 ext4_file_write_iter+0x54/0x704 vfs_write+0x1c0/0x308 ksys_write+0x74/0x10c __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x114 el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x40/0xe4 el0t_64_sync_handler+0x120/0x12c el0t_64_sync+0x194/0x198 Root cause is: systemd-random-seed kworker ---------- ___mark_inode_dirty inode_switch_wbs_work_fn spin_lock(&inode->i_lock); inode_attach_wb locked_inode_to_wb_and_lock_list get inode->i_wb spin_unlock(&inode->i_lock); spin_lock(&wb->list_lock) spin_lock(&inode->i_lock) inode_io_list_move_locked spin_unlock(&wb->list_lock) spin_unlock(&inode->i_lock) spin_lock(&old_wb->list_lock) inode_do_switch_wbs spin_lock(&inode->i_lock) inode->i_wb = new_wb spin_unlock(&inode->i_lock) spin_unlock(&old_wb->list_lock) wb_put_many(old_wb, nr_switched) cgwb_release old wb released wb_wakeup_delayed() accesses wb, then trigger the use-after-free issue Fix this race condition by holding inode spinlock until wb_wakeup_delayed() finished.	N/A	More Details
CVE-2025-10156	An Improper Handling of Exceptional Conditions vulnerability in the ZIP archive scanning component of mmaitre314 picklescan allows a remote attacker to bypass security scans. This is achieved by crafting a ZIP archive containing a file with a bad Cyclic Redundancy Check (CRC), which causes the scanner to halt and fail to analyze the contents for malicious pickle files. When the file incorrectly considered safe is loaded, it can lead to the execution of malicious code.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ppp: fix memory leak in pad_compress_skb		

CVE-2025-39847	If alloc_skb() fails in pad_compress_skb(), it returns NULL without releasing the old skb. The caller does: skb = pad_compress_skb(ppp, skb); if (!skb) goto drop; drop: kfree_skb(skb); When pad_compress_skb() returns NULL, the reference to the old skb is lost and kfree_skb(skb) ends up doing nothing, leading to a memory leak. Align pad_compress_skb() semantics with realloc(): only free the old skb if allocation and compression succeed. At the call site, use the new_skb variable so the original skb is not lost when pad_compress_skb() fails.	N/A	More Details
CVE-2025-6921	The huggingface/transformers library, versions prior to 4.53.0, is vulnerable to Regular Expression Denial of Service (ReDoS) in the AdamWeightDecay optimizer. The vulnerability arises from the _do_use_weight_decay method, which processes user-controlled regular expressions in the include_in_weight_decay and exclude_from_weight_decay lists. Malicious regular expressions can cause catastrophic backtracking during the re.search call, leading to 100% CPU utilization and a denial of service. This issue can be exploited by attackers who can control the patterns in these lists, potentially causing the machine learning task to hang and rendering services unresponsive.	N/A	More Details
CVE-2025-39859	In the Linux kernel, the following vulnerability has been resolved: ptp: ocp: fix use-after-free bugs causing by ptp_ocp_watchdog The ptp_ocp_detach() only shuts down the watchdog timer if it is pending. However, if the timer handler is already running, the timer_delete_sync() is not called. This leads to race conditions where the devlink that contains the ptp_ocp is deallocated while the timer handler is still accessing it, resulting in use-after-free bugs. The following details one of the race scenarios. (thread 1) | (thread 2) ptp_ocp_remove() | ptp_ocp_detach() | ptp_ocp_watchdog() if (timer_pending(&bp->watchdog))| bp = timer_container_of() timer_delete_sync() | | devlink_free(devlink) //free | | bp-> //use Resolve this by unconditionally calling timer_delete_sync() to ensure the timer is reliably deactivated, preventing any access after free.	N/A	More Details
CVE-2025-9242	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer.This vulnerability affects Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.3 and 2025.1.	N/A	More Details
CVE-2025-10184	The vulnerability allows any application installed on the device to read SMS/MMS data and metadata from the system-provided Telephony provider without permission, user interaction, or consent. The user is also not notified that SMS data is being accessed. This could lead to sensitive information disclosure and could effectively break the security provided by SMS-based Multi-Factor Authentication (MFA) checks. The root cause is a combination of missing permissions for write operations in several content providers (com.android.providers.telephony.PushMessageProvider, com.android.providers.telephony.PushShopProvider, com.android.providers.telephony.ServiceNumberProvider), and a blind SQL injection in the update method of those providers.	N/A	More Details
CVE-2025-59825	astral-tokio-tar is a tar archive reading/writing library for async Rust. In versions 0.5.3 and earlier of astral-tokio-tar, tar archives may extract outside of their intended destination directory when using the Entry::unpack_in_raw API. Additionally, the Entry::allow_external_symlinks control (which defaults to true) could be bypassed via a pair of symlinks that individually point within the destination but combine to point outside of it. These behaviors could be used individually or combined to bypass the intended security control of limiting extraction to the given directory. This in turn would allow an attacker with a malicious tar archive to perform an arbitrary file write and potentially pivot into code execution. This issue has been patched in version 0.5.4. There is no workaround other than upgrading.	N/A	More Details
CVE-2025-8153	Cross-site Scripting vulnerability in NEC Corporation UNIVERGE IX from Ver.9.5 to Ver.10.7, from Ver.10.8.21 to Ver.10.8.36, from Ver.10.9.11 to Ver.10.9.24, from Ver.10.10.21 to Ver.10.10.31, Ver.10.11.6 and UNIVERGE IX-R/IX-V Ver1.3.16, Ver1.3.21 allows a attacker to inject an arbitrary scripts may be executed on the user's browser.	N/A	More Details
CVE-2025-39850	In the Linux kernel, the following vulnerability has been resolved: vxlan: Fix NPD in {arp,neigh}_reduce() when using nexthop objects When the "proxy" option is enabled on a VXLAN device, the device will suppress ARP requests and IPv6 Neighbor Solicitation messages if it is able to reply on behalf of the remote host. That is, if a matching and valid neighbor entry is configured on the VXLAN device whose MAC address is not behind the "any" remote (0.0.0.0 / ::). The code currently assumes that the FDB entry for the neighbor's MAC address points to a valid remote destination, but this is incorrect if the entry is associated with an FDB nexthop group. This can result in a NPD [1][3] which can be reproduced using [2][4]. Fix by checking that the remote destination exists before dereferencing it. [1] BUG: kernel NULL pointer dereference, address: 0000000000000000 [...] CPU: 4 UID: 0 PID: 365 Comm: arping Not tainted 6.17.0-rc2-virtme-g2a89cb21162c #2 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-4.fc41 04/01/2014 RIP: 0010:vxlan_xmit+0xb58/0x15f0 [...] Call Trace: <TASK> dev_hard_start_xmit+0x5d/0x1c0 __dev_queue_xmit+0x246/0xfd0 packet_sendmsg+0x113a/0x1850 __sock_sendmsg+0x38/0x70 __sys_sendto+0x126/0x180 __x64_sys_sendto+0x24/0x30 do_syscall_64+0xa4/0x260 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [2] #!/bin/bash ip address add 192.0.2.1/32 dev lo ip nexthop add id 1 via 192.0.2.2 fdb ip nexthop add id 10 group 1 fdb ip link add name vx0 up type vxlan id 10010 local 192.0.2.1 dstport 4789 proxy ip neigh add 192.0.2.3 lladdr 00:11:22:33:44:55 nud perm dev vx0 bridge fdb add 00:11:22:33:44:55 dev vx0 self static nhid 10 arping -b -c 1 -s 192.0.2.1 -I vx0 192.0.2.3 [3] BUG: kernel NULL pointer dereference, address: 0000000000000000 [...] CPU: 13 UID: 0 PID: 372 Comm: ndisc6 Not tainted 6.17.0-rc2-virtmne-g6ee90cb26014 #3 PREEMPT(voluntary) Hardware name: QEMU Standard PC	N/A	More Details

	(i440FX + PIIX, 1v996), BIOS 1.17.0-4.fc41 04/01/2x014 RIP: 0010:vxlan_xmit+0x803/0x1600 [...] Call Trace: <TASK> dev_hard_start_xmit+0x5d/0x1c0 __dev_queue_xmit+0x246/0xfd0 ip6_finish_output2+0x210/0x6c0 ip6_finish_output+0x1af/0x2b0 ip6_mr_output+0x92/0x3e0 ip6_send_skb+0x30/0x90 rawv6_sendmsg+0xe6e/0x12e0 __sock_sendmsg+0x38/0x70 __sys_sendto+0x126/0x180 __x64_sys_sendto+0x24/0x30 do_syscall_64+0xa4/0x260 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f383422ec77 [4] #!/bin/bash ip address add 2001:db8:1::1/128 dev lo ip nexthop add id 1 via 2001:db8:1::1 fdb ip nexthop add id 10 group 1 fdb ip link add name vx0 up type vxlan id 10010 local 2001:db8:1::1 dstport 4789 proxy ip neigh add 2001:db8:1::3 lladdr 00:11:22:33:44:55 nud perm dev vx0 bridge fdb add 00:11:22:33:44:55 dev vx0 self static nhid 10 ndisc6 -r 1 -s 2001:db8:1::1 -w 1 2001:db8:1::3 vx0		
CVE-2025-39851	In the Linux kernel, the following vulnerability has been resolved: vxlan: Fix NPD when refreshing an FDB entry with a nexthop object VXLAN FDB entries can point to either a remote destination or an FDB nexthop group. The latter is usually used in EVPN deployments where learning is disabled. However, when learning is enabled, an incoming packet might try to refresh an FDB entry that points to an FDB nexthop group and therefore does not have a remote. Such packets should be dropped, but they are only dropped after dereferencing the non-existent remote, resulting in a NPD [1] which can be reproduced using [2]. Fix by dropping such packets earlier. Remove the misleading comment from first_remote_rcu(). [1] BUG: kernel NULL pointer dereference, address: 0000000000000000 [...] CPU: 13 UID: 0 PID: 361 Comm: mausezahn Not tainted 6.17.0-rc1-virtme-g9f6b606b6b37 #1 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-4.fc41 04/01/2014 RIP: 0010:vxlan_snoop+0x98/0x1e0 [...] Call Trace: <TASK> vxlan_encap_bypass+0x209/0x240 encap_bypass_if_local+0xb1/0x100 vxlan_xmit_one+0x1375/0x17e0 vxlan_xmit+0x6b4/0x15f0 dev_hard_start_xmit+0x5d/0x1c0 __dev_queue_xmit+0x246/0xfd0 packet_sendmsg+0x113a/0x1850 __sock_sendmsg+0x38/0x70 __sys_sendto+0x126/0x180 __x64_sys_sendto+0x24/0x30 do_syscall_64+0xa4/0x260 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [2] #!/bin/bash ip address add 192.0.2.1/32 dev lo ip address add 192.0.2.2/32 dev lo ip nexthop add id 1 via 192.0.2.3 fdb ip nexthop add id 10 group 1 fdb ip link add name vx0 up type vxlan id 10010 local 192.0.2.1 dstport 12345 localbypass ip link add name vx1 up type vxlan id 10020 local 192.0.2.2 dstport 54321 learning bridge fdb add 00:11:22:33:44:55 dev vx0 self static dst 192.0.2.2 port 54321 vni 10020 bridge fdb add 00:aa:bb:cc:dd:ee dev vx1 self static nhid 10 mausezahn vx0 -a 00:aa:bb:cc:dd:ee -b 00:11:22:33:44:55 -c 1 -q	N/A	More Details
CVE-2025-39852	In the Linux kernel, the following vulnerability has been resolved: net/tcp: Fix socket memory leak in TCP-AO failure handling for IPv6 When tcp_ao_copy_all_matching() fails in tcp_v6_syn_recv_sock() it just exits the function. This ends up causing a memory-leak: unreferenced object 0xffff0000281a8200 (size 2496): comm "softirq", pid 0, jiffies 4295174684 hex dump (first 32 bytes): 7f 00 00 06 7f 00 00 06 00 00 00 00 cb a8 88 13 ..... 0a 00 03 61 00 00 00 00 00 00 00 00 00 00 00 00 ...a..... backtrace (crc 5ebdbe15): kmemleak_alloc+0x44/0xe0 kmem_cache_alloc_noprof+0x248/0x470 sk_prot_alloc+0x48/0x120 sk_clone_lock+0x38/0x3b0 inet_csk_clone_lock+0x34/0x150 tcp_create_openreq_child+0x3c/0x4a8 tcp_v6_syn_recv_sock+0x1c0/0x620 tcp_check_req+0x588/0x790 tcp_v6_rcv+0x5d0/0xc18 ip6_protocol_deliver_rcu+0x2d8/0x4c0 ip6_input_finish+0x74/0x148 ip6_input+0x50/0x118 ip6_sublist_rcv+0x2fc/0x3b0 ipv6_list_rcv+0x114/0x170 __netif_receive_skb_list_core+0x16c/0x200 netif_receive_skb_list_internal+0x1f0/0x2d0 This is because in tcp_v6_syn_recv_sock (and the IPv4 counterpart), when exiting upon error, inet_csk_prepare_forced_close() and tcp_done() need to be called. They make sure the newsk will end up being correctly free'd. tcp_v4_syn_recv_sock() makes this very clear by having the put_and_exit label that takes care of things. So, this patch here makes sure tcp_v4_syn_recv_sock and tcp_v6_syn_recv_sock have similar error-handling and thus fixes the leak for TCP-AO.	N/A	More Details
CVE-2025-39853	In the Linux kernel, the following vulnerability has been resolved: i40e: Fix potential invalid access when MAC list is empty list_first_entry() never returns NULL - if the list is empty, it still returns a pointer to an invalid object, leading to potential invalid memory access when dereferenced. Fix this by using list_first_entry_or_null instead of list_first_entry.	N/A	More Details
CVE-2025-39854	In the Linux kernel, the following vulnerability has been resolved: ice: fix NULL access of tx->in_use in ice_ll_ts_intr Recent versions of the E810 firmware have support for an extra interrupt to handle report of the "low latency" Tx timestamps coming from the specialized low latency firmware interface. Instead of polling the registers, software can wait until the low latency interrupt is fired. This logic makes use of the Tx timestamp tracking structure, ice_ptp_tx, as it uses the same "ready" bitmap to track which Tx timestamps complete. Unfortunately, the ice_ll_ts_intr() function does not check if the tracker is initialized before its first access. This results in NULL dereference or use-after-free bugs similar to the issues fixed in the ice_ptp_ts_irq() function. Fix this by only checking the in_use bitmap (and other fields) if the tracker is marked as initialized. The reset flow will clear the init field under lock before it tears the tracker down, thus preventing any use-after-free or NULL access.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: ice: fix NULL access of tx->in_use in ice_ptp_ts_irq The E810 device has support for a "low latency" firmware interface to access and read the Tx timestamps. This interface does not use the standard Tx timestamp logic, due to the latency overhead of proxying sideband command requests over the firmware AdminQ. The logic still makes use of the Tx timestamp tracking structure, ice_ptp_tx, as it uses the same "ready" bitmap to track which Tx timestamps		

2025-39855	complete. Unfortunately, the ice_ptp_ts_irq() function does not check if the tracker is initialized before its first access. This results in NULL dereference or use-after-free bugs similar to the following: [245977.278756] BUG: kernel NULL pointer dereference, address: 0000000000000000 [245977.278774] RIP: 0010:_find_first_bit+0x19/0x40 [245977.278796] Call Trace: [245977.278809] ? ice_misc_intr+0x364/0x380 [ice] This can occur if a Tx timestamp interrupt races with the driver reset logic. Fix this by only checking the in_use bitmap (and other fields) if the tracker is marked as initialized. The reset flow will clear the init field under lock before it tears the tracker down, thus preventing any use-after-free or NULL access.	N/A	More Details
CVE-2025-39856	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: am65-cpsw-nuss: Fix null pointer dereference for ndev In the TX completion packet stage of TI SoCs with CPSW2G instance, which has single external ethernet port, ndev is accessed without being initialized if no TX packets have been processed. It results into null pointer dereference, causing kernel to crash. Fix this by having a check on the number of TX packets which have been processed.	N/A	More Details
CVE-2025-58354	Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. In Kata Containers versions from 3.20.0 and before, a malicious host can circumvent initdata verification. On TDX systems running confidential guests, a malicious host can selectively fail IO operations to skip initdata verification. This allows an attacker to launch arbitrary workloads while being able to attest successfully to Trustee impersonating any benign workload. This issue has been patched in Kata Containers version 3.21.0.	N/A	More Details
CVE-2025-56311	In Shenzhen C-Data Technology Co. FD602GW-DX-R410 (firmware v2.2.14), the web management interface contains an authenticated CSRF vulnerability on the reboot endpoint (/boaform/admin/formReboot). An attacker can craft a malicious webpage that, when visited by an authenticated administrator, causes the router to reboot without explicit user consent. This lack of CSRF protection on a sensitive administrative function can lead to denial of service by disrupting network availability.	N/A	More Details
CVE-2025-57636	OS Command injection vulnerability in D-Link C1 2020-02-21. The sub_47F028 function in jhttpd contains a command injection vulnerability via the HTTP parameter "time".	N/A	More Details
CVE-2025-8410	Use After Free vulnerability in RTI Connext Professional (Security Plugins) allows File Manipulation.This issue affects Connext Professional: from 7.5.0 before 7.6.0.	N/A	More Details
CVE-2025-59822	Http4s is a Scala interface for HTTP services. In versions from 1.0.0-M1 to before 1.0.0-M45 and before 0.23.31, http4s is vulnerable to HTTP Request Smuggling due to improper handling of HTTP trailer section. This vulnerability could enable attackers to bypass front-end servers security controls, launch targeted attacks against active users, and poison web caches. A pre-requisite for exploitation involves the web application being deployed behind a reverse-proxy that forwards trailer headers. This issue has been patched in versions 1.0.0-M45 and 0.23.31.	N/A	More Details
CVE-2025-39857	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix one NULL pointer dereference in smc_ib_is_sg_need_sync() BUG: kernel NULL pointer dereference, address: 00000000000002ec PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP PTI CPU: 28 UID: 0 PID: 343 Comm: kworker/28:1 Kdump: loaded Tainted: G OE 6.17.0-rc2+ #9 NONE Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 Workqueue: smc_hs_wq smc_listen_work [smc] RIP: 0010:smc_ib_is_sg_need_sync+0x9e/0xd0 [smc] ... Call Trace: <TASK> smcr_buf_map_link+0x211/0x2a0 [smc] __smc_buf_create+0x522/0x970 [smc] smc_buf_create+0x3a/0x110 [smc] smc_find_rdma_v2_device_serv+0x18f/0x240 [smc] ? smc_vlan_by_tcpsk+0x7e/0xe0 [smc] smc_listen_find_device+0x1dd/0x2b0 [smc] smc_listen_work+0x30f/0x580 [smc] process_one_work+0x18c/0x340 worker_thread+0x242/0x360 kthread+0xe7/0x220 ret_from_fork+0x13a/0x160 ret_from_fork_asm+0x1a/0x30 </TASK> If the software RoCE device is used, ibdev->dma_device is a null pointer. As a result, the problem occurs. Null pointer detection is added to prevent problems.	N/A	More Details
CVE-2025-59307	RAID Manager provided by Century Corporation registers a Windows service with an unquoted file path. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2025-57638	Buffer overflow vulnerability in Tenda AC9 1.0 via the user supplied sys.vendor configuration value.	N/A	More Details
CVE-2025-57637	Buffer overflow vulnerability in D-Link DI-7100G 2020-02-21 in the sub_451754 function of the jhttpd service in the viav4 parameter allowing attackers to cause a denial of service or execute arbitrary code.	N/A	More Details
CVE-2025-56146	Indian Bank IndSMART Android App 3.8.1 is vulnerable to Missing SSL Certificate Validation in NuWebViewActivity.	N/A	More Details

CVE-2025-39858	In the Linux kernel, the following vulnerability has been resolved: eth: mlx4: Fix IS_ERR() vs NULL check bug in mlx4_en_create_rx_ring Replace NULL check with IS_ERR() check after calling page_pool_create() since this function returns error pointers (ERR_PTR). Using NULL check could lead to invalid pointer dereference.	N/A	More Details
CVE-2025-51005	A heap-buffer-overflow vulnerability exists in the tcpliveplay utility of the tcpreplay-4.5.1. When a crafted pcap file is processed, the program incorrectly handles memory in the checksum calculation logic at do_checksum_math_liveplay in tcpliveplay.c, leading to a possible denial of service.	N/A	More Details
CVE-2025-45326	An issue in PocketVJ CP PocketVJ-CP-v3 pvj 3.9.1 allows remote attackers to execute arbitrary code via the submit_size.php component.	N/A	More Details
CVE-2025-9197	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-39846	In the Linux kernel, the following vulnerability has been resolved: pcmcia: Fix a NULL pointer dereference in __iodyn_find_io_region() In __iodyn_find_io_region(), pcmcia_make_resource() is assigned to res and used in pci_bus_alloc_resource(). There is a dereference of res in pci_bus_alloc_resource(), which could lead to a NULL pointer dereference on failure of pcmcia_make_resource(). Fix this bug by adding a check of res.	N/A	More Details
CVE-2025-9966	Improper privilege management vulnerability in Novakon P series allows attackers to gain root privileges if one service is compromized.This issue affects P series: P – V2001.A.C518o2.	N/A	More Details
CVE-2025-59885	Rejected reason: Not used	N/A	More Details
CVE-2025-39867	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo: fix null deref for empty set Blamed commit broke the check for a null scratch map: - if (unlikely(!m || !*raw_cpu_ptr(m->scratch))) + if (unlikely(!raw_cpu_ptr(m->scratch))) This should have been "if (!*raw_ ...)". Use the pattern of the avx2 version which is more readable. This can only be reproduced if avx2 support isn't available.	N/A	More Details
CVE-2025-39877	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: fix use-after-free in state_show() state_show() reads kdamond->damon_ctx without holding damon_sysfs_lock. This allows a use-after-free race: CPU 0 CPU 1 ----- ----- state_show() damon_sysfs_turn_damon_on() ctx = kdamond->damon_ctx; mutex_lock(&damon_sysfs_lock); damon_destroy_ctx(kdamond->damon_ctx); kdamond->damon_ctx = NULL; mutex_unlock(&damon_sysfs_lock); damon_is_running(ctx); /* ctx is freed */ mutex_lock(&ctx->kdamond_lock); /* UAF */ (The race can also occur with damon_sysfs_kdamonds_rm_dirs() and damon_sysfs_kdamond_release(), which free or replace the context under damon_sysfs_lock.) Fix by taking damon_sysfs_lock before dereferencing the context, mirroring the locking used in pid_show(). The bug has existed since state_show() first accessed kdamond->damon_ctx.	N/A	More Details
CVE-2025-39876	In the Linux kernel, the following vulnerability has been resolved: net: fec: Fix possible NPD in fec_enet_phy_reset_after_clk_enable() The function of_phy_find_device may return NULL, so we need to take care before dereferencing phy_dev.	N/A	More Details
CVE-2025-39875	In the Linux kernel, the following vulnerability has been resolved: igb: Fix NULL pointer dereference in ethtool loopback test The igb driver currently causes a NULL pointer dereference when executing the ethtool loopback test. This occurs because there is no associated q_vector for the test ring when it is set up, as interrupts are typically not added to the test rings. Since commit 5ef44b3cb43b removed the napi_id assignment in __xdp_rxq_info_reg(), there is no longer a need to pass a napi_id to it. Therefore, simply use 0 as the last parameter.	N/A	More Details
CVE-2025-39874	In the Linux kernel, the following vulnerability has been resolved: macsec: sync features on RTM_NEWLINK Syzkaller managed to lock the lower device via ETHTOOL_SFEATURES: netdev_lock include/linux/netdevice.h:2761 [inline] netdev_lock_ops include/net/netdev_lock.h:42 [inline] netdev_sync_lower_features net/core/dev.c:10649 [inline] __netdev_update_features+0xcb1/0x1be0 net/core/dev.c:10819 netdev_update_features+0x6d/0xe0 net/core/dev.c:10876 macsec_notify+0x2f5/0x660 drivers/net/macsec.c:4533 notifier_call_chain+0x1b3/0x3e0 kernel/notifier.c:85 call_netdevice_notifiers_extack net/core/dev.c:2267 [inline] call_netdevice_notifiers net/core/dev.c:2281 [inline] netdev_features_change+0x85/0xc0 net/core/dev.c:1570 __dev_ethtool net/ethtool/ioctl.c:3469 [inline] dev_ethtool+0x1536/0x19b0 net/ethtool/ioctl.c:3502 dev_ioctl+0x392/0x1150 net/core/dev_ioctl.c:759 It happens because lower features are out of sync with the upper: __dev_ethtool (real_dev) netdev_lock_ops(real_dev) ETHTOOL_SFEATURES __netdev_features_change netdev_sync_upper_features disable LRO on the lower if (old_features != dev->features) netdev_features_change fires NETDEV_FEAT_CHANGE macsec_notify NETDEV_FEAT_CHANGE netdev_update_features (for each macsec dev) netdev_sync_lower_features if (upper_features != lower_features) netdev_lock_ops(lower) # lower == real_dev stuck ... netdev_unlock_ops(real_dev) Per commit af5f54b0ef9e ("net: Lock lower level devices when updating features"), we elide the lock/unlock when the upper and lower features are synced. Makes sure the lower (real_dev) has proper features after the	N/A	More Details

	macsec link has been created. This makes sure we never hit the situation where we need to sync upper flags to the lower.		
CVE-2025-39873	In the Linux kernel, the following vulnerability has been resolved: can: xilinx_can: xcan_write_frame(): fix use-after-free of transmitted SKB can_put_echo_skb() takes ownership of the SKB and it may be freed during or after the call. However, xilinx_can xcan_write_frame() keeps using SKB after the call. Fix that by only calling can_put_echo_skb() after the code is done touching the SKB. The tx_lock is held for the entire xcan_write_frame() execution and also on the can_get_echo_skb() side so the order of operations does not matter. An earlier fix commit 3d3c817c3a40 ("can: xilinx_can: Fix usage of skb memory") did not move the can_put_echo_skb() call far enough. [mkl: add "commit" in front of sha1 in patch description] [mkl: fix indention]	N/A	More Details
CVE-2025-39872	In the Linux kernel, the following vulnerability has been resolved: hsr: hold rcu and dev lock for hsr_get_port_ndev hsr_get_port_ndev calls hsr_for_each_port, which need to hold rcu lock. On the other hand, before return the port device, we need to hold the device reference to avoid UaF in the caller function.	N/A	More Details
CVE-2025-39871	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Remove improper idxd_free The call to idxd_free() introduces a duplicate put_device() leading to a reference count underflow: refcount_t: underflow; use-after-free. WARNING: CPU: 15 PID: 4428 at lib/refcount.c:28 refcount_warn_saturate+0xbe/0x110 ... Call Trace: <TASK> idxd_remove+0xe4/0x120 [idxd] pci_device_remove+0x3f/0xb0 device_release_driver_internal+0x197/0x200 driver_detach+0x48/0x90 bus_remove_driver+0x74/0xf0 pci_unregister_driver+0x2e/0xb0 idxd_exit_module+0x34/0x7a0 [idxd] __do_sys_delete_module.constprop.0+0x183/0x280 do_syscall_64+0x54/0xd70 entry_SYSCALL_64_after_hwframe+0x76/0x7e The idxd_unregister_devices() which is invoked at the very beginning of idxd_remove(), already takes care of the necessary put_device() through the following call path: idxd_unregister_devices() -> device_unregister() -> put_device() In addition, when CONFIG_DEBUG_KOBJECT_RELEASE is enabled, put_device() may trigger asynchronous cleanup via schedule_delayed_work(). If idxd_free() is called immediately after, it can result in a use-after-free. Remove the improper idxd_free() to avoid both the refcount underflow and potential memory corruption during module unload.	N/A	More Details
CVE-2025-39870	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix double free in idxd_setup_wqs() The clean up in idxd_setup_wqs() has had a couple bugs because the error handling is a bit subtle. It's simpler to just re-write it in a cleaner way. The issues here are: 1) If "idxd->max_wqs" is <= 0 then we call put_device(conf_dev) when "conf_dev" hasn't been initialized. 2) If kzalloc_node() fails then again "conf_dev" is invalid. It's either uninitialized or it points to the "conf_dev" from the previous iteration so it leads to a double free. It's better to free partial loop iterations within the loop and then the unwinding at the end can handle whole loop iterations. I also renamed the labels to describe what the goto does and not where the goto was located.	N/A	More Details
CVE-2025-39869	In the Linux kernel, the following vulnerability has been resolved: dmaengine: ti: edma: Fix memory allocation size for queue_priority_map Fix a critical memory allocation bug in edma_setup_from_hw() where queue_priority_map was allocated with insufficient memory. The code declared queue_priority_map as s8 (*)[2] (pointer to array of 2 s8), but allocated memory using sizeof(s8) instead of the correct size. This caused out-of-bounds memory writes when accessing: queue_priority_map[i][0] = i; queue_priority_map[i][1] = i; The bug manifested as kernel crashes with "Oops - undefined instruction" on ARM platforms (BeagleBoard-X15) during EDMA driver probe, as the memory corruption triggered kernel hardening features on Clang. Change the allocation to use sizeof(*queue_priority_map) which automatically gets the correct size for the 2D array structure.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: erofs: fix runtime warning on truncate_folio_batch_exceptionals() Commit 0e2f80afcfa6("fs/dax: ensure all pages are idle prior to filesystem unmount") introduced the WARN_ON_ONCE to capture whether the filesystem has removed all DAX entries or not and applied the fix to xfs and ext4. Apply the missed fix on erofs to fix the runtime warning: [5.266254] ------------[cut here]------------ [5.266274] WARNING: CPU: 6 PID: 3109 at mm/truncate.c:89 truncate_folio_batch_exceptionals+0xff/0x260 [5.266294] Modules linked in: [5.266999] CPU: 6 UID: 0 PID: 3109 Comm: umount Tainted: G S 6.16.0+ #6 PREEMPT(voluntary) [5.267012] Tainted: [S]=CPU_OUT_OF_SPEC [5.267017] Hardware name: Dell Inc. OptiPlex 5000/05WXFV, BIOS 1.5.1 08/24/2022 [5.267024] RIP: 0010:truncate_folio_batch_exceptionals+0xff/0x260 [5.267076] Code: 00 00 41 39 df 7f 11 eb 78 83 c3 01 49 83 c4 08 41 39 df 74 6c 48 63 f3 48 83 fe 1f 0f 83 3c 01 00 00 43 f6 44 26 08 01 74 df <0f> 0b 4a 8b 34 22 4c 89 ef 48 89 55 90 e8 ff 54 1f 00 48 8b 55 90 [5.267083] RSP: 0018:ffffc900013f36c8 EFLAGS: 00010202 [5.267095] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000 [5.267101] RDX: ffffc900013f3790 RSI: 0000000000000000 RDI: ffff8882a1407898 [5.267108] RBP: ffffc900013f3740 R08: 0000000000000000 R09: 0000000000000000 [5.267113] R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000 [5.267119] R13: ffff8882a1407ab8 R14: ffffc900013f3888 R15: 0000000000000001 [5.267125] FS: 00007aaa8b437800(0000) GS:ffff88850025b000(0000) knlGS:0000000000000000 [5.267132] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [5.267138] CR2: 00007aaa8b3aac10 CR3: 000000024f764000 CR4: 0000000000f52ef0 [5.267144] PKRU: 55555554 [5.267150] Call Trace: [5.267154] <TASK> [5.267181] truncate_inode_pages_range+0x118/0x5e0 [5.267193] ? save_trace+0x54/0x390 [5.267296] truncate_inode_pages_final+0x43/0x60 [5.267309] evict+0x2a4/0x2c0 [5.267339] dispose_list+0x39/0x80 [	More

2025-39868	5.267352] evict_inodes+0x150/0x1b0 [5.267376] generic_shutdown_super+0x41/0x180 [5.267390] kill_block_super+0x1b/0x50 [5.267402] erofs_kill_sb+0x81/0x90 [erofs] [5.267436] deactivate_locked_super+0x32/0xb0 [5.267450] deactivate_super+0x46/0x60 [5.267460] cleanup_mnt+0xc3/0x170 [5.267475] __cleanup_mnt+0x12/0x20 [5.267485] task_work_run+0x5d/0xb0 [5.267499] exit_to_user_mode_loop+0x144/0x170 [5.267512] do_syscall_64+0x2b9/0x7c0 [5.267523] ? __lock_acquire+0x665/0x2ce0 [5.267535] ? __lock_acquire+0x665/0x2ce0 [5.267560] ? lock_acquire+0xcd/0x300 [5.267573] ? find_held_lock+0x31/0x90 [5.267582] ? mntput_no_expire+0x97/0x4e0 [5.267606] ? mntput_no_expire+0xa1/0x4e0 [5.267625] ? mntput+0x24/0x50 [5.267634] ? path_put+0x1e/0x30 [5.267647] ? do_faccessat+0x120/0x2f0 [5.267677] ? do_syscall_64+0x1a2/0x7c0 [5.267686] ? from_kgid_munged+0x17/0x30 [5.267703] ? from_kuid_munged+0x13/0x30 [5.267711] ? __do_sys_getuid+0x3d/0x50 [5.267724] ? do_syscall_64+0x1a2/0x7c0 [5.267732] ? irqentry_exit+0x77/0xb0 [5.267743] ? clear_bhb_loop+0x30/0x80 [5.267752] ? clear_bhb_loop+0x30/0x80 [5.267765] entry_SYSCALL_64_after_hwframe+0x76/0x7e [5.267772] RIP: 0033:0x7aaa8b32a9fb [5.267781] Code: c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 f3 0f 1e fa 31 f6 e9 05 00 00 00 0f 1f 44 00 00 f3 0f 1e fa b8 a6 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 05 c3 0f 1f 40 00 48 8b 15 e9 83 0d 00 f7 d8 [5.267787] RSP: 002b:00007ffd7c4c9468 EFLAGS: 00000246 ORIG_RAX: 00000000000000a6 [5.267796] RAX: 0000000000000000 RBX: 00005a61592a8b00 RCX: 00007aaa8b32a9fb [5.267802] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 00005a61592b2080 [5.267806] RBP: 00007ffd7c4c9540 R08: 00007aaa8b403b20 R09: 0000000000000020 [5.267812] R10: 0000000000000001 R11: 0000000000000246 R12: 00005a61592a8c00 [5.267817] R13: 00000000 ---truncated---	N/A	Details
CVE-2025-59476	Jenkins 2.527 and earlier, LTS 2.516.2 and earlier does not restrict or transform the characters that can be inserted from user-specified content in log messages, allowing attackers able to control log message contents to insert line break characters, followed by forged log messages that may mislead administrators reviewing log output.	N/A	More Details
CVE-2025-39879	In the Linux kernel, the following vulnerability has been resolved: ceph: always call ceph_shift_unused_folios_left() The function ceph_process_folio_batch() sets folio_batch entries to NULL, which is an illegal state. Before folio_batch_release() crashes due to this API violation, the function ceph_shift_unused_folios_left() is supposed to remove those NULLs from the array. However, since commit ce80b76dd327 ("ceph: introduce ceph_process_folio_batch() method"), this shifting doesn't happen anymore because the "for" loop got moved to ceph_process_folio_batch(), and now the `i` variable that remains in ceph_writepages_start() doesn't get incremented anymore, making the shifting effectively unreachable much of the time. Later, commit 1551ec61dc55 ("ceph: introduce ceph_submit_write() method") added more preconditions for doing the shift, replacing the `i` check (with something that is still just as broken): - if ceph_process_folio_batch() fails, shifting never happens - if ceph_move_dirty_page_in_page_array() was never called (because ceph_process_folio_batch() has returned early for some of various reasons), shifting never happens - if `processed_in_fbatch` is zero (because ceph_process_folio_batch() has returned early for some of the reasons mentioned above or because ceph_move_dirty_page_in_page_array() has failed), shifting never happens Since those two commits, any problem in ceph_process_folio_batch() could crash the kernel, e.g. this way: BUG: kernel NULL pointer dereference, address: 0000000000000034 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: Oops: 0002 [#1] SMP NOPTI CPU: 172 UID: 0 PID: 2342707 Comm: kworker/u778:8 Not tainted 6.15.10-cm4all1-es #714 NONE Hardware name: Dell Inc. PowerEdge R7615/0G9DHV, BIOS 1.6.10 12/08/2023 Workqueue: writeback wb_workfn (flush-ceph-1) RIP: 0010:folios_put_refs+0x85/0x140 Code: 83 c5 01 39 e8 7e 76 48 63 c5 49 8b 5c c4 08 b8 01 00 00 00 4d 85 ed 74 05 41 8b 44 ad 00 48 8b 15 b0 > RSP: 0018:ffffb880af8db778 EFLAGS: 00010207 RAX: 0000000000000001 RBX: 0000000000000000 RCX: 0000000000000003 RDX: ffffe377cc3b0000 RSI: 0000000000000000 RDI: ffffb880af8db8c0 RBP: 0000000000000000 R08: 000000000000007d R09: 000000000102b86f R10: 0000000000000001 R11: 00000000000000ac R12: ffffb880af8db8c0 R13: 0000000000000000 R14: 0000000000000000 R15: ffff9bd262c97000 FS: 0000000000000000(0000) GS:ffff9c8efc303000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000034 CR3: 0000000160958004 CR4: 0000000000770ef0 PKRU: 55555554 Call Trace: <TASK> ceph_writepages_start+0xeb9/0x1410 The crash can be reproduced easily by changing the ceph_check_page_before_write() return value to `-E2BIG`. (Interestingly, the crash happens only if `huge_zero_folio` has already been allocated; without `huge_zero_folio`, is_huge_zero_folio(NULL) returns true and folios_put_refs() skips NULL entries instead of dereferencing them. That makes reproducing the bug somewhat unreliable. See https://lore.kernel.org/20250826231626.218675-1-max.kellermann@ionos.com for a discussion of this detail.) My suggestion is to move the ceph_shift_unused_folios_left() to right after ceph_process_folio_batch() to ensure it always gets called to fix up the illegal folio_batch state.	N/A	More Details
CVE-2022-50353	In the Linux kernel, the following vulnerability has been resolved: mmc: wmt-sdmmc: fix return value check of mmc_add_host() mmc_add_host() may return error, if we ignore its return value, the memory that allocated in mmc_alloc_host() will be leaked and it will lead a kernel crash because of deleting not added device in the remove path. So fix this by checking the return value and goto error path which will call mmc_free_host(), besides, clk_disable_unprepare() also needs be called.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix kfd_process_device_init_vm error handling Should only destroy the ib_mem and let process cleanup worker to		

CVE-2022-50354	free the outstanding BOs. Reset the pointer in pdd->qpd structure, to avoid NULL pointer access in process destroy worker. BUG: kernel NULL pointer dereference, address: 0000000000000010 Call Trace: amdgpu_amdkfd_gpuvm_unmap_gtt_bo_from_kernel+0x46/0xb0 [amdgpu] kfd_process_device_destroy_cwsr_dgpu+0x40/0x70 [amdgpu] kfd_process_destroy_pdds+0x71/0x190 [amdgpu] kfd_process_wq_release+0x2a2/0x3b0 [amdgpu] process_one_work+0x2a1/0x600 worker_thread+0x39/0x3d0	N/A	More Details
CVE-2025-1131	A local privilege escalation vulnerability exists in the safe_asterisk script included with the Asterisk toolkit package. When Asterisk is started via this script (common in SysV init or FreePBX environments), it sources all .sh files located in /etc/asterisk/startup.d/ as root, without validating ownership or permissions. Non-root users with legitimate write access to /etc/asterisk can exploit this behaviour by placing malicious scripts in the startup.d directory, which will then execute with root privileges upon service restart.	N/A	More Details
CVE-2022-50355	In the Linux kernel, the following vulnerability has been resolved: staging: vt6655: fix some erroneous memory clean-up loops In some initialization functions of this driver, memory is allocated with 'i' acting as an index variable and increasing from 0. The commit in "Fixes" introduces some clean-up codes in case of allocation failure, which free memory in reverse order with 'i' decreasing to 0. However, there are some problems: - The case i=0 is left out. Thus memory is leaked. - In case memory allocation fails right from the start, the memory freeing loops will start with i=-1 and invalid memory locations will be accessed. One of these loops has been fixed in commit c8ff91535880 ("staging: vt6655: fix potential memory leak"). Fix the remaining erroneous loops.	N/A	More Details
CVE-2022-50356	In the Linux kernel, the following vulnerability has been resolved: net: sched: sfb: fix null pointer access issue when sfb_init() fails When the default qdisc is sfb, if the qdisc of dev_queue fails to be inited during mqprio_init(), sfb_reset() is invoked to clear resources. In this case, the q->qdisc is NULL, and it will cause gpf issue. The process is as follows: qdisc_create_dflt() sfb_init() tcf_block_get() --->failed, q->qdisc is NULL ... qdisc_put() ... sfb_reset() qdisc_reset(q->qdisc) --->q->qdisc is NULL ops = qdisc->ops The following is the Call Trace information: general protection fault, probably for non-canonical address 0xdfffffc0000000003: 0000 [#1] PREEMPT SMP KASAN KASAN: null-ptr-deref in range [0x0000000000000018-0x000000000000001f] RIP: 0010:qdisc_reset+0x2b/0x6f0 Call Trace: <TASK> sfb_reset+0x37/0xd0 qdisc_reset+0xed/0x6f0 qdisc_destroy+0x82/0x4c0 qdisc_put+0x9e/0xb0 qdisc_create_dflt+0x2c3/0x4a0 mqprio_init+0xa71/0x1760 qdisc_create+0x3eb/0x1000 tc_modify_qdisc+0x408/0x1720 rtnetlink_rcv_msg+0x38e/0xac0 netlink_rcv_skb+0x12d/0x3a0 netlink_unicast+0x4a2/0x740 netlink_sendmsg+0x826/0xcc0 sock_sendmsg+0xc5/0x100 ____sys_sendmsg+0x583/0x690 ___sys_sendmsg+0xe8/0x160 __sys_sendmsg+0xbf/0x160 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 RIP: 0033:0x7f2164122d04 </TASK>	N/A	More Details
CVE-2022-50357	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: core: fix some leaks in probe The dwc3_get_properties() function calls: dwc->usb_psy = power_supply_get_by_name(usb_psy_name); so there is some additional clean up required on these error paths.	N/A	More Details
CVE-2022-50358	In the Linux kernel, the following vulnerability has been resolved: brcmfmac: return error when getting invalid max_flowrings from dongle When firmware hit trap at initialization, host will read abnormal max_flowrings number from dongle, and it will cause kernel panic when doing iowrite to initialize dongle ring. To detect this error at early stage, we directly return error when getting invalid max_flowrings(>256).	N/A	More Details
CVE-2022-50359	In the Linux kernel, the following vulnerability has been resolved: media: cx88: Fix a null-ptr-deref bug in buffer_prepare() When the driver calls cx88_risc_buffer() to prepare the buffer, the function call may fail, resulting in a empty buffer and null-ptr-deref later in buffer_queue(). The following log can reveal it: [41.822762] general protection fault, probably for non-canonical address 0xdfffffc0000000000: 0000 [#1] PREEMPT SMP KASAN PTI [41.824488] KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] [41.828027] RIP: 0010:buffer_queue+0xc2/0x500 [41.836311] Call Trace: [41.836945] __enqueue_in_driver+0x141/0x360 [41.837262] vb2_start_streaming+0x62/0x4a0 [41.838216] vb2_core_streamon+0x1da/0x2c0 [41.838516] __vb2_init_fileio+0x981/0xbc0 [41.839141] __vb2_perform_fileio+0xbf9/0x1120 [41.840072] vb2_fop_read+0x20e/0x400 [41.840346] v4l2_read+0x215/0x290 [41.840603] vfs_read+0x162/0x4c0 Fix this by checking the return value of cx88_risc_buffer() [hverkuil: fix coding style issues]	N/A	More Details
CVE-2025-9862	Server-Side Request Forgery (SSRF) vulnerability in Ghost allows an attacker to access internal resources.This issue affects Ghost: from 6.0.0 through 6.0.8, from 5.99.0 through 5.130.3.	N/A	More Details
CVE-2022-50361	In the Linux kernel, the following vulnerability has been resolved: wifi: wilc1000: add missing unregister_netdev() in wilc_netdev_ifc_init() Fault injection test reports this issue: kernel BUG at net/core/dev.c:10731! invalid opcode: 0000 [#1] PREEMPT SMP KASAN PTI Call Trace: <TASK> wilc_netdev_ifc_init+0x19f/0x220 [wilc1000 884bf126e9e98af6a708f266a8dffd53f99e4bf5] wilc_cfg80211_init+0x30c/0x380 [wilc1000 884bf126e9e98af6a708f266a8dffd53f99e4bf5] wilc_bus_probe+0xad/0x2b0 [wilc1000_spi 1520a7539b6589cc6cde2ae826a523a33f8bacff] spi_probe+0xe4/0x140 really_probe+0x17e/0x3f0 __driver_probe_device+0xe3/0x170 driver_probe_device+0x49/0x120 The root case here is alloc_ordered_workqueue() fails, but cfg80211_unregister_netdevice() or unregister_netdev() not be called in error handling path. To fix add	N/A	More Details

	unregister_netdev goto lable to add the unregister operation in error handling path.		
CVE-2025-39878	In the Linux kernel, the following vulnerability has been resolved: ceph: fix crash after fscrypt_encrypt_pagecache_blocks() error The function move_dirty_folio_in_page_array() was created by commit ce80b76dd327 ("ceph: introduce ceph_process_folio_batch() method") by moving code from ceph_writepages_start() to this function. This new function is supposed to return an error code which is checked by the caller (now ceph_process_folio_batch()), and on error, the caller invokes redirty_page_for_writepage() and then breaks from the loop. However, the refactoring commit has gone wrong, and it by accident, it always returns 0 (= success) because it first NULLs the pointer and then returns PTR_ERR(NULL) which is always 0. This means errors are silently ignored, leaving NULL entries in the page array, which may later crash the kernel. The simple solution is to call PTR_ERR() before clearing the pointer.	N/A	More Details
CVE-2025-39880	In the Linux kernel, the following vulnerability has been resolved: libceph: fix invalid accesses to ceph_connection_v1_info There is a place where generic code in messenger.c is reading and another place where it is writing to con->v1 union member without checking that the union member is active (i.e. msgr1 is in use). On 64-bit systems, con->v1.auth_retry overlaps with con->v2.out_iter, so such a read is almost guaranteed to return a bogus value instead of 0 when msgr2 is in use. This ends up being fairly benign because the side effect is just the invalidation of the authorizer and successive fetching of new tickets. con->v1.connect_seq overlaps with con->v2.conn_bufs and the fact that it's being written to can cause more serious consequences, but luckily it's not something that happens often.	N/A	More Details
CVE-2025-9965	Improper authentication vulnerability in Novakon P series allows unauthenticated attackers to upload and download any application from/to the device.This issue affects P series: P – V2001.A.C518o2.	N/A	More Details
CVE-2025-39843	In the Linux kernel, the following vulnerability has been resolved: mm: slub: avoid wake up kswapd in set_track_prepare set_track_prepare() can incur lock recursion. The issue is that it is called from hrtimer_start_range_ns holding the per_cpu(hrtimer_bases)[n].lock, but when enabled CONFIG_DEBUG_OBJECTS_TIMERS, may wake up kswapd in set_track_prepare, and try to hold the per_cpu(hrtimer_bases)[n].lock. Avoid deadlock caused by implicitly waking up kswapd by passing in allocation flags, which do not contain __GFP_KSWAPD_RECLAIM in the debug_objects_fill_pool() case. Inside stack depot they are processed by gfp_nested_mask(). Since ___slab_alloc() has preemption disabled, we mask out __GFP_DIRECT_RECLAIM from the flags there. The oops looks something like: BUG: spinlock recursion on CPU#3, swapper/3/0 lock: 0xffffff8a4bf29c80, .magic: dead4ead, .owner: swapper/3/0, .owner_cpu: 3 Hardware name: Qualcomm Technologies, Inc. Popsicle based on SM8850 (DT) Call trace: spin_bug+0x0 _raw_spin_lock_irqsave+0x80 hrtimer_try_to_cancel+0x94 task_contending+0x10c enqueue_dl_entity+0x2a4 dl_server_start+0x74 enqueue_task_fair+0x568 enqueue_task+0xac do_activate_task+0x14c ttwu_do_activate+0xcc try_to_wake_up+0x6c8 default_wake_function+0x20 autoremove_wake_function+0x1c __wake_up+0xac wakeup_kswapd+0x19c wake_all_kswapds+0x78 __alloc_pages_slowpath+0x1ac __alloc_pages_noprof+0x298 stack_depot_save_flags+0x6b0 stack_depot_save+0x14 set_track_prepare+0x5c ___slab_alloc+0xccc __kmalloc_cache_noprof+0x470 __set_page_owner+0x2bc post_alloc_hook[jt]+0x1b8 prep_new_page+0x28 get_page_from_freelist+0x1edc __alloc_pages_noprof+0x13c alloc_slab_page+0x244 allocate_slab+0x7c ___slab_alloc+0x8e8 kmem_cache_alloc_noprof+0x450 debug_objects_fill_pool+0x22c debug_object_activate+0x40 enqueue_hrtimer[jt]+0xdc hrtimer_start_range_ns+0x5f8 ...	N/A	More Details
CVE-2025-9964	No password for the root user is set in Novakon P series. This allows phyiscal attackers to enter the console easily. This issue affects P series: P – V2001.A.C518o2.	N/A	More Details
CVE-2025-9963	A path traversal vulnerability in Novakon P series allows to expose the root file system "/" and modify all files with root permissions. This way the system can also be compromized.This issue affects P series: P – V2001.A.C518o2.	N/A	More Details
CVE-2025-9962	A buffer overflow vulnerability in Novakon P series allows attackers to gain root permission without prior authentication.This issue affects P series: P – V2001.A.C518o2.	N/A	More Details
CVE-2025-39845	In the Linux kernel, the following vulnerability has been resolved: x86/mm/64: define ARCH_PAGE_TABLE_SYNC_MASK and arch_sync_kernel_mappings() Define ARCH_PAGE_TABLE_SYNC_MASK and arch_sync_kernel_mappings() to ensure page tables are properly synchronized when calling p*d_populate_kernel(). For 5-level paging, synchronization is performed via pgd_populate_kernel(). In 4-level paging, pgd_populate() is a no-op, so synchronization is instead performed at the P4D level via p4d_populate_kernel(). This fixes intermittent boot failures on systems using 4-level paging and a large amount of persistent memory: BUG: unable to handle page fault for address: ffffe70000000034 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] SMP NOPTI RIP: 0010:__init_single_page+0x9/0x6d Call Trace: <TASK> __init_zone_device_page+0x17/0x5d memmap_init_zone_device+0x154/0x1bb pagemap_range+0x2e0/0x40f memremap_pages+0x10b/0x2f0 devm_memremap_pages+0x1e/0x60 dev_dax_probe+0xce/0x2ec [device_dax] dax_bus_probe+0x6d/0xc9 [... snip ...] </TASK> It also fixes a crash in vmemmap_set_pmd() caused by accessing vmemmap before sync_global_pgds() [1]: BUG: unable to handle page fault for address: ffffeb3ff1200000 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page	N/A	More Details

	PGD 0 P4D 0 Oops: Oops: 0002 [#1] PREEMPT SMP NOPTI Tainted: [W]=WARN RIP: 0010:vmemmap_set_pmd+0xff/0x230 <TASK> vmemmap_populate_hugepages+0x176/0x180 vmemmap_populate+0x34/0x80 __populate_section_memmap+0x41/0x90 sparse_add_section+0x121/0x3e0 __add_pages+0xba/0x150 add_pages+0x1d/0x70 memremap_pages+0x3dc/0x810 devm_memremap_pages+0x1c/0x60 xe_devm_add+0x8b/0x100 [xe] xe_tile_init_noalloc+0x6a/0x70 [xe] xe_device_probe+0x48c/0x740 [xe] [... snip ...]		
CVE-2025-10157	A Protection Mechanism Failure vulnerability in mmaitre314 picklescan versions up to and including 0.0.30 allows a remote attacker to bypass the unsafe globals check. This is possible because the scanner performs an exact match for module names, allowing malicious payloads to be loaded via submodules of dangerous packages (e.g., 'asyncio.unix_events' instead of 'asyncio'). When the incorrectly considered safe file is loaded after scan, it can lead to the execution of malicious code.	N/A	More Details
CVE-2025-7106	danny-avila/librechat is affected by an authorization bypass vulnerability due to improper access control checks. The `checkAccess` function in `api/server/middleware/roles/access.js` uses `permissions.some()` to validate permissions, which incorrectly grants access if only one of multiple required permissions is present. This allows users with the 'USER' role to create agents despite having `CREATE: false` permission, as the check for `['USE', 'CREATE']` passes with just `USE: true`. This vulnerability affects other permission checks as well, such as `PROMPTS`. The issue is present in all versions prior to the fix.	N/A	More Details
CVE-2025-59427	The Cloudflare Vite plugin enables a full-featured integration between Vite and the Workers runtime. When utilising the Cloudflare Vite plugin in its default configuration, all files are exposed by the local dev server, including files in the root directory that contain secret information such as .env and .dev.vars. This vulnerability is fixed in 1.6.0.	N/A	More Details
CVE-2022-4980	General Bytes Crypto Application Server (CAS) beginning with version 20201208 prior to 20220531.38 (backport) and 20220725.22 (mainline) contains an authentication bypass in the admin web interface. An unauthenticated attacker could invoke the same URL used by the product's default-installation / first-admin creation page and create a new administrative account remotely. By gaining admin privileges, the attacker can change the ATM configuration resulting in redirected funds. Public vendor advisories and multiple independent writeups describe the vulnerability as a call to the page used for initial/default installation / first administration user creation; General Bytes has not publicly published the exact endpoint/parameter name. The issue was actively exploited in the wild against cloud-hosted and standalone CAS deployments (scanning exposed CAS instances on ports 7777/443), and publicly acknowledged by the General Bytes in September 2022.	N/A	More Details
CVE-2024-13990	MicroWorld eScan AV's update mechanism failed to ensure authenticity and integrity of updates: update packages were delivered and accepted without robust cryptographic verification. As a result, an on-path attacker could perform a man-in-the-middle (MitM) attack and substitute malicious update payloads for legitimate ones. The eScan AV client accepted these substituted packages and executed or loaded their components (including sideloaded DLLs and Java/installer payloads), enabling remote code execution on affected systems. MicroWorld eScan confirmed remediation of the update mechanism on 2023-07-31 but versioning details are unavailable. NOTE: MicroWorld eScan disputes the characterization in third-party reports, stating the issue relates to 2018–2019 and that controls were implemented then.	N/A	More Details
CVE-2025-39844	In the Linux kernel, the following vulnerability has been resolved: mm: move page table sync declarations to linux/pgtable.h During our internal testing, we started observing intermittent boot failures when the machine uses 4-level paging and has a large amount of persistent memory: BUG: unable to handle page fault for address: ffffe70000000034 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] SMP NOPTI RIP: 0010:__init_single_page+0x9/0x6d Call Trace: <TASK> __init_zone_device_page+0x17/0x5d memmap_init_zone_device+0x154/0x1bb pagemap_range+0x2e0/0x40f memremap_pages+0x10b/0x2f0 devm_memremap_pages+0x1e/0x60 dev_dax_probe+0xce/0x2ec [device_dax] dax_bus_probe+0x6d/0xc9 [... snip ...] </TASK> It turns out that the kernel panics while initializing vmemmap (struct page array) when the vmemmap region spans two PGD entries, because the new PGD entry is only installed in init_mm.pgd, but not in the page tables of other tasks. And looking at __populate_section_memmap(): if (vmemmap_can_optimize(altmap, pgmap)) // does not sync top level page tables r = vmemmap_populate_compound_pages(pfn, start, end, nid, pgmap); else // sync top level page tables in x86 r = vmemmap_populate(start, end, nid, altmap); In the normal path, vmemmap_populate() in arch/x86/mm/init_64.c synchronizes the top level page table (See commit 9b861528a801 ("x86-64, mem: Update all PGDs for direct mapping and vmemmap mapping changes")) so that all tasks in the system can see the new vmemmap area. However, when vmemmap_can_optimize() returns true, the optimized path skips synchronization of top-level page tables. This is because vmemmap_populate_compound_pages() is implemented in core MM code, which does not handle synchronization of the top-level page tables. Instead, the core MM has historically relied on each architecture to perform this synchronization manually. We're not the first party to encounter a crash caused by not-sync'd top level page tables: earlier this year, Gwan-gyeong Mun attempted to address the issue [1] [2] after hitting a kernel panic when x86 code accessed the vmemmap area before the corresponding top-level entries were synced. At that time, the issue was believed to be triggered only when struct page was enlarged for debugging purposes, and the patch did not get further updates. It turns out that current approach of relying on each arch to handle the page table sync manually is fragile because 1) it's easy to forget to sync the top level page table, and 2) it's also easy to overlook that the kernel should not access the vmemmap and direct	N/A	More Details

	mapping areas before the sync. # The solution: Make page table sync more code robust and harder to miss To address this, Dave Hansen suggested [3] [4] introducing {pgd,p4d}_populate_kernel() for updating kernel portion of the page tables and allow each architecture to explicitly perform synchronization when installing top-level entries. With this approach, we no longer need to worry about missing the sync step, reducing the risk of future regressions. The new interface reuses existing ARCH_PAGE_TABLE_SYNC_MASK, PGTBL_P*D_MODIFIED and arch_sync_kernel_mappings() facility used by vmalloc and ioremap to synchronize page tables. pgd_populate_kernel() looks like this: static inline void pgd_populate_kernel(unsigned long addr, pgd_t *pgd, p4d_t *p4d) { pgd_populate(&init_mm, pgd, p4d); if (ARCH_PAGE_TABLE_SYNC_MASK & PGTBL_PGD_MODIFIED) arch_sync_kernel_mappings(addr, addr); } It is worth noting that vmalloc() and apply_to_range() carefully synchronizes page tables by calling p*d_alloc_track() and arch_sync_kernel_mappings(), and thus they are not affected by ---truncated---		
CVE-2025-34188	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 1.0.735 and Application prior to 20.0.1330 (macOS/Linux client deployments) contain a vulnerability in the local logging mechanism. Authentication session tokens, including PHPSESSID, XSRF-TOKEN, and laravel_session, are stored in cleartext within world-readable log files. Any local user with access to the machine can extract these session tokens and use them to authenticate remotely to the SaaS environment, bypassing normal login credentials, potentially leading to unauthorized system access and exposure of sensitive information.	N/A	More Details
CVE-2025-39881	In the Linux kernel, the following vulnerability has been resolved: kernfs: Fix UAF in polling when open file is released A use-after-free (UAF) vulnerability was identified in the PSI (Pressure Stall Information) monitoring mechanism: BUG: KASAN: slab-use-after-free in psi_trigger_poll+0x3c/0x140 Read of size 8 at addr ffff3de3d50bd308 by task systemd/1 psi_trigger_poll+0x3c/0x140 cgroup_pressure_poll+0x70/0xa0 cgroup_file_poll+0x8c/0x100 kernfs_fop_poll+0x11c/0x1c0 ep_item_poll.isra.0+0x188/0x2c0 Allocated by task 1: cgroup_file_open+0x88/0x388 kernfs_fop_open+0x73c/0xaf0 do_dentry_open+0x5fc/0x1200 vfs_open+0xa0/0x3f0 do_open+0x7e8/0xd08 path_openat+0x2fc/0x6b0 do_filp_open+0x174/0x368 Freed by task 8462: cgroup_file_release+0x130/0x1f8 kernfs_drain_open_files+0x17c/0x440 kernfs_drain+0x2dc/0x360 kernfs_show+0x1b8/0x288 cgroup_file_show+0x150/0x268 cgroup_pressure_write+0x1dc/0x340 cgroup_file_write+0x274/0x548 Reproduction Steps: 1. Open test/cpu.pressure and establish epoll monitoring 2. Disable monitoring: echo 0 > test/cgroup.pressure 3. Re-enable monitoring: echo 1 > test/cgroup.pressure The race condition occurs because: 1. When cgroup.pressure is disabled (echo 0 > cgroup.pressure), it: - Releases PSI triggers via cgroup_file_release() - Frees of->priv through kernfs_drain_open_files() 2. While epoll still holds reference to the file and continues polling 3. Re-enabling (echo 1 > cgroup.pressure) accesses freed of->priv epolling disable/enable cgroup.pressure fd=open(cpu.pressure) while(1) ... epoll_wait kernfs_fop_poll kernfs_get_active = true echo 0 > cgroup.pressure ... cgroup_file_show kernfs_show // inactive kn kernfs_drain_open_files cft->release(of); kfree(ctx); ... kernfs_get_active = false echo 1 > cgroup.pressure kernfs_show kernfs_activate_one(kn); kernfs_fop_poll kernfs_get_active = true cgroup_file_poll psi_trigger_poll // UAF ... end: close(fd) To address this issue, introduce kernfs_get_active_of() for kernfs open files to obtain active references. This function will fail if the open file has been released. Replace kernfs_get_active() with kernfs_get_active_of() to prevent further operations on released file descriptors.	N/A	More Details
CVE-2025-34189	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 1.0.735 and Application versions prior to 20.0.1330 (macOS/Linux client deployments) contain a vulnerability in the local inter-process communication (IPC) mechanism. The software stores IPC request and response files inside /opt/PrinterInstallerClient/tmp with world-readable and world-writable permissions. Any local user can craft malicious request files that are processed by privileged daemons, leading to unauthorized actions being executed in other user sessions. This breaks user session isolation, potentially allowing local attackers to hijack sessions, perform unintended actions in the context of other users, and impact system integrity and availability.	N/A	More Details
CVE-2025-59474	Jenkins 2.527 and earlier, LTS 2.516.2 and earlier does not perform a permission check in the sidepanel of a page intentionally accessible to users lacking Overall/Read permission, allowing attackers without Overall/Read permission to list agent names through its sidepanel executors widget.	N/A	More Details
CVE-2025-59475	Jenkins 2.527 and earlier, LTS 2.516.2 and earlier does not perform a permission check for the authenticated user profile dropdown menu, allowing attackers without Overall/Read permission to obtain limited information about the Jenkins configuration by listing available options in this menu (e.g., whether Credentials Plugin is installed).	N/A	More Details
CVE-2025-39888	In the Linux kernel, the following vulnerability has been resolved: fuse: Block access to folio overlimit syz reported a slab-out-of-bounds Write in fuse_dev_do_write. When the number of bytes to be retrieved is truncated to the upper limit by fc->max_pages and there is an offset, the oob is triggered. Add a loop termination condition to prevent overruns.	N/A	More Details
CVE-2025-39887	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Fix null-ptr-deref in bitmap_parselist() A crash was observed with the following output: BUG: kernel NULL pointer dereference, address: 0000000000000010 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 2 UID: 0 PID: 92 Comm: osnoise_cpus Not tainted 6.17.0-rc4-00201-gd69eb204c255 #138 PREEMPT(voluntary) RIP: 0010:bitmap_parselist+0x53/0x3e0 Call Trace: <TASK> osnoise_cpus_write+0x7a/0x190 vfs_write+0xf8/0x410 ? do_sys_openat2+0x88/0xd0 ksys_write+0x60/0xd0 do_syscall_64+0xa4/0x260	N/A	More Details

	entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> This issue can be reproduced by below code: fd=open("/sys/kernel/debug/tracing/osnoise/cpus", O_WRONLY); write(fd, "0-2", 0); When user pass 'count=0' to osnoise_cpus_write(), kmalloc() will return ZERO_SIZE_PTR (16) and cpulist_parse() treat it as a normal value, which trigger the null pointer dereference. Add check for the parameter 'count'.		
CVE-2025-39886	In the Linux kernel, the following vulnerability has been resolved: bpf: Tell memcg to use allow_spinning=false path in bpf_timer_init() Currently, calling bpf_map_kmalloc_node() from __bpf_async_init() can cause various locking issues; see the following stack trace (edited for style) as one example: ... [10.011566] do_raw_spin_lock.cold [10.011570] try_to_wake_up (5) double-acquiring the same [10.011575] kick_pool rq_lock, causing a hardlockup [10.011579] __queue_work [10.011582] queue_work_on [10.011585] kernfs_notify [10.011589] cgroup_file_notify [10.011593] try_charge_memcg (4) memcg accounting raises an [10.011597] obj_cgroup_charge_pages MEMCG_MAX event [10.011599] obj_cgroup_charge_account [10.011600] __memcg_slab_post_alloc_hook [10.011603] __kmalloc_node_noprof ... [10.011611] bpf_map_kmalloc_node [10.011612] __bpf_async_init [10.011615] bpf_timer_init (3) BPF calls bpf_timer_init() [10.011617] bpf_prog_xxxxxxxxxxxxxxxx_fcg_runnable [10.011619] bpf__sched_ext_ops_runnable [10.011620] enqueue_task_scx (2) BPF runs with rq_lock held [10.011622] enqueue_task [10.011626] ttwu_do_activate [10.011629] sched_ttwu_pending (1) grabs rq_lock ... The above was reproduced on bpf-next (b338cf849ec8) by modifying ./tools/sched_ext/scx_flatcg.bpf.c to call bpf_timer_init() during ops.runnable(), and hacking the memcg accounting code a bit to make a bpf_timer_init() call more likely to raise an MEMCG_MAX event. We have also run into other similar variants (both internally and on bpf-next), including double-acquiring cgroup_file_kn_lock, the same worker_pool::lock, etc. As suggested by Shakeel, fix this by using __GFP_HIGH instead of GFP_ATOMIC in __bpf_async_init(), so that e.g. if try_charge_memcg() raises an MEMCG_MAX event, we call __memcg_memory_event() with @allow_spinning=false and avoid calling cgroup_file_notify() there. Depends on mm patch "memcg: skip cgroup_file_notify if spinning is not allowed": https://lore.kernel.org/bpf/20250905201606.66198-1-shakeel.butt@linux.dev/ v0 approach s/bpf_map_kmalloc_node/bpf_mem_alloc/ https://lore.kernel.org/bpf/20250905061919.439648-1-yepeilin@google.com/ v1 approach: https://lore.kernel.org/bpf/20250905234547.862249-1-yepeilin@google.com/	N/A	More Details
CVE-2025-39885	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix recursive semaphore deadlock in fiemap call syzbot detected a OCFS2 hang due to a recursive semaphore on a FS_IOC_FIEMAP of the extent list on a specially crafted mmap file. context_switch kernel/sched/core.c:5357 [inline] __schedule+0x1798/0x4cc0 kernel/sched/core.c:6961 __schedule_loop kernel/sched/core.c:7043 [inline] schedule+0x165/0x360 kernel/sched/core.c:7058 schedule_preempt_disabled+0x13/0x30 kernel/sched/core.c:7115 rwsem_down_write_slowpath+0x872/0xfe0 kernel/locking/rwsem.c:1185 __down_write_common kernel/locking/rwsem.c:1317 [inline] __down_write kernel/locking/rwsem.c:1326 [inline] down_write+0x1ab/0x1f0 kernel/locking/rwsem.c:1591 ocfs2_page_mkwrite+0x2ff/0xc40 fs/ocfs2/mmap.c:142 do_page_mkwrite+0x14d/0x310 mm/memory.c:3361 wp_page_shared mm/memory.c:3762 [inline] do_wp_page+0x268d/0x5800 mm/memory.c:3981 handle_pte_fault mm/memory.c:6068 [inline] __handle_mm_fault+0x1033/0x5440 mm/memory.c:6195 handle_mm_fault+0x40a/0x8e0 mm/memory.c:6364 do_user_addr_fault+0x764/0x1390 arch/x86/mm/fault.c:1387 handle_page_fault arch/x86/mm/fault.c:1476 [inline] exc_page_fault+0x76/0xf0 arch/x86/mm/fault.c:1532 asm_exc_page_fault+0x26/0x30 arch/x86/include/asm/idtentry.h:623 RIP: 0010:copy_user_generic arch/x86/include/asm/uaccess_64.h:126 [inline] RIP: 0010:raw_copy_to_user arch/x86/include/asm/uaccess_64.h:147 [inline] RIP: 0010:_inline_copy_to_user include/linux/uaccess.h:197 [inline] RIP: 0010:_copy_to_user+0x85/0xb0 lib/usercopy.c:26 Code: e8 00 bc f7 fc 4d 39 fc 72 3d 4d 39 ec 77 38 e8 91 b9 f7 fc 4c 89 f7 89 de e8 47 25 5b fd 0f 01 cb 4c 89 ff 48 89 d9 4c 89 f6 <f3> a4 0f 1f 00 48 89 cb 0f 01 ca 48 89 d8 5b 41 5c 41 5d 41 5e 41 RSP: 0018:ffffc9000403f950 EFLAGS: 00050256 RAX: ffffffff84c7f101 RBX: 0000000000000038 RCX: 0000000000000038 RDX: 0000000000000000 RSI: ffffc9000403f9e0 RDI: 0000200000000060 RBP: ffffc9000403fa90 R08: ffffc9000403fa17 R09: 1ffff92000807f42 R10: dfffffc0000000000 R11: fffff52000807f43 R12: 0000200000000098 R13: 00007fffffffff000 R14: ffffc9000403f9e0 R15: 0000200000000060 copy_to_user include/linux/uaccess.h:225 [inline] fiemap_fill_next_extent+0x1c0/0x390 fs/ioctl.c:145 ocfs2_fiemap+0x888/0xc90 fs/ocfs2/extent_map.c:806 ioctl_fiemap fs/ioctl.c:220 [inline] do_vfs_ioctl+0x1173/0x1430 fs/ioctl.c:532 __do_sys_ioctl fs/ioctl.c:596 [inline] __se_sys_ioctl+0x82/0x170 fs/ioctl.c:584 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f5f13850fd9 RSP: 002b:00007ffe3b3518b8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 0000200000000000 RCX: 00007f5f13850fd9 RDX: 0000200000000040 RSI: 00000000c020660b RDI: 0000000000000004 RBP: 6165627472616568 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffe3b3518f0 R13: 00007ffe3b351b18 R14: 431bde82d7b634db R15: 00007f5f1389a03b ocfs2_fiemap() takes a read lock of the ip_alloc_sem semaphore (since v2.6.22-527-g7307de80510a) and calls fiemap_fill_next_extent() to read the extent list of this running mmap executable. The user supplied buffer to hold the fiemap information page faults calling ocfs2_page_mkwrite() which will take a write lock (since v2.6.27-38-g00dc417fa3e7) of the same semaphore. This recursive semaphore will hold filesystem locks and causes a hang of the fileystem. The ip_alloc_sem protects the inode extent list and size. Release the read semphore before calling fiemap_fill_next_extent() in ocfs2_fiemap() and ocfs2_fiemap_inline(). This does an unnecessary semaphore lock/unlock on the last extent but simplifies the error path.	N/A	More Details

CVE-2025-39884	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix subvolume deletion lockup caused by inodes xarray race There is a race condition between inode eviction and inode caching that can cause a live struct btrfs_inode to be missing from the root->inodes xarray. Specifically, there is a window during evict() between the inode being unhashed and deleted from the xarray. If btrfs_iget() is called for the same inode in that window, it will be recreated and inserted into the xarray, but then eviction will delete the new entry, leaving nothing in the xarray: Thread 1 Thread 2 ---------- evict() remove_inode_hash() btrfs_iget_path() btrfs_iget_locked() btrfs_read_locked_inode() btrfs_add_inode_to_root() destroy_inode() btrfs_destroy_inode() btrfs_del_inode_from_root() __xa_erase In turn, this can cause issues for subvolume deletion. Specifically, if an inode is in this lost state, and all other inodes are evicted, then btrfs_del_inode_from_root() will call btrfs_add_dead_root() prematurely. If the lost inode has a delayed_node attached to it, then when btrfs_clean_one_deleted_snapshot() calls btrfs_kill_all_delayed_nodes(), it will loop forever because the delayed_nodes xarray will never become empty (unless memory pressure forces the inode out). We saw this manifest as soft lockups in production. Fix it by only deleting the xarray entry if it matches the given inode (using __xa_cmpxchg()).	N/A	More Details
CVE-2025-39883	In the Linux kernel, the following vulnerability has been resolved: mm/memory-failure: fix VM_BUG_ON_PAGE(PagePoisoned(page)) when unpoison memory When I did memory failure tests, below panic occurs: page dumped because: VM_BUG_ON_PAGE(PagePoisoned(page)) kernel BUG at include/linux/page-flags.h:616! Oops: invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 720 Comm: bash Not tainted 6.10.0-rc1-00195-g148743902568 #40 RIP: 0010:unpoison_memory+0x2f3/0x590 RSP: 0018:ffffa57fc8787d60 EFLAGS: 00000246 RAX: 0000000000000037 RBX: 0000000000000009 RCX: ffff9be25fcdc9c8 RDX: 0000000000000000 RSI: 0000000000000027 RDI: ffff9be25fcdc9c0 RBP: 0000000000300000 R08: ffffffffb4956f88 R09: 0000000000009ffb R10: 0000000000000284 R11: ffffffffb4926fa0 R12: ffffe6b00c000000 R13: ffff9bdb453dfd00 R14: 0000000000000000 R15: fffffffffffffffe FS: 00007f08f04e4740(0000) GS:ffff9be25fcc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000564787a30410 CR3: 000000010d4e2000 CR4: 00000000000006f0 Call Trace: <TASK> unpoison_memory+0x2f3/0x590 simple_attr_write_xsigned.constprop.0.isra.0+0xb3/0x110 debugfs_attr_write+0x42/0x60 full_proxy_write+0x5b/0x80 vfs_write+0xd5/0x540 ksys_write+0x64/0xe0 do_syscall_64+0xb9/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f08f0314887 RSP: 002b:00007ffece710078 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 0000000000000009 RCX: 00007f08f0314887 RDX: 0000000000000009 RSI: 0000564787a30410 RDI: 0000000000000001 RBP: 0000564787a30410 R08: 000000000000fefe R09: 000000007fffffff R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000009 R13: 00007f08f041b780 R14: 00007f08f0417600 R15: 00007f08f0416a00 </TASK> Modules linked in: hwpoison_inject ---[end trace 0000000000000000]--- RIP: 0010:unpoison_memory+0x2f3/0x590 RSP: 0018:ffffa57fc8787d60 EFLAGS: 00000246 RAX: 0000000000000037 RBX: 0000000000000009 RCX: ffff9be25fcdc9c8 RDX: 0000000000000000 RSI: 0000000000000027 RDI: ffff9be25fcdc9c0 RBP: 0000000000300000 R08: ffffffffb4956f88 R09: 0000000000009ffb R10: 0000000000000284 R11: ffffffffb4926fa0 R12: ffffe6b00c000000 R13: ffff9bdb453dfd00 R14: 0000000000000000 R15: fffffffffffffffe FS: 00007f08f04e4740(0000) GS:ffff9be25fcc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000564787a30410 CR3: 000000010d4e2000 CR4: 00000000000006f0 Kernel panic - not syncing: Fatal exception Kernel Offset: 0x31c00000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff) ---[end Kernel panic - not syncing: Fatal exception]--- The root cause is that unpoison_memory() tries to check the PG_HWPoison flags of an uninitialized page. So VM_BUG_ON_PAGE(PagePoisoned(page)) is triggered. This can be reproduced by below steps: 1.Offline memory block: echo offline > /sys/devices/system/memory/memory12/state 2.Get offlined memory pfn: page-types -b n -rlN 3.Write pfn to unpoison-pfn echo <pfn> > /sys/kernel/debug/hwpoison/unpoison-pfn This scenario can be identified by pfn_to_online_page() returning NULL. And ZONE_DEVICE pages are never expected, so we can simply fail if pfn_to_online_page() == NULL to fix the bug.	N/A	More Details
CVE-2025-39882	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: fix potential OF node use-after-free The for_each_child_of_node() helper drops the reference it takes to each node as it iterates over children and an explicit of_node_put() is only needed when exiting the loop early. Drop the recently introduced bogus additional reference count decrement at each iteration that could potentially lead to a use-after-free.	N/A	More Details
CVE-2023-53368	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix race issue between cpu buffer write and swap Warning happened in rb_end_commit() at code: if (RB_WARN_ON(cpu_buffer, !local_read(&cpu_buffer->committing))) WARNING: CPU: 0 PID: 139 at kernel/trace/ring_buffer.c:3142 rb_commit+0x402/0x4a0 Call Trace: ring_buffer_unlock_commit+0x42/0x250 trace_buffer_unlock_commit_regs+0x3b/0x250 trace_event_buffer_commit+0xe5/0x440 trace_event_buffer_reserve+0x11c/0x150 trace_event_raw_event_sched_switch+0x23c/0x2c0 __traceiter_sched_switch+0x59/0x80 __schedule+0x72b/0x1580 schedule+0x92/0x120 worker_thread+0xa0/0x6f0 It is because the race between writing event into cpu buffer and swapping cpu buffer through file per_cpu/cpu0/snapshot: Write on CPU 0 Swap buffer by per_cpu/cpu0/snapshot on CPU 1 ---------- -------- tracing_snapshot_write() [...] ring_buffer_lock_reserve() cpu_buffer = buffer->buffers[cpu]; // 1. Suppose find 'cpu_buffer_a'; [...] rb_reserve_next_event() [...] ring_buffer_swap_cpu() if (local_read(&cpu_buffer_a->committing)) goto out_dec; if (local_read(&cpu_buffer_b->committing)) goto out_dec; buffer_a->buffers[cpu] = cpu_buffer_b; buffer_b->buffers[cpu] = cpu_buffer_a; // 2. cpu_buffer has swapped here. rb_start_commit(cpu_buffer); if (unlikely(READ_ONCE(cpu_buffer->buffer) != buffer)) { // 3.	N/A	More Details

	This check passed due to 'cpu_buffer->buffer' [...] // has not changed here. return NULL; } cpu_buffer_b->buffer = buffer_a; cpu_buffer_a->buffer = buffer_b; [...] // 4. Reserve event from 'cpu_buffer_a'. ring_buffer_unlock_commit() [...] cpu_buffer = buffer->buffers[cpu]; // 5. Now find 'cpu_buffer_b' !!! rb_commit(cpu_buffer) rb_end_commit() // 6. WARN for the wrong 'committing' state !!! Based on above analysis, we can easily reproduce by following testcase: ``` bash #!/bin/bash dmesg -n 7 sysctl -w kernel.panic_on_warn=1 TR=/sys/kernel/tracing echo 7 > ${TR}/buffer_size_kb echo "sched:sched_switch" > ${TR}/set_event while [true]; do echo 1 > ${TR}/per_cpu/cpu0/snapshot done & while [true]; do echo 1 > ${TR}/per_cpu/cpu0/snapshot done & while [true]; do echo 1 > ${TR}/per_cpu/cpu0/snapshot done & ``` To fix it, IIUC, we can use smp_call_function_single() to do the swap on the target cpu where the buffer is located, so that above race would be avoided.		
CVE-2023-53405	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: gr_udc: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2025-39840	In the Linux kernel, the following vulnerability has been resolved: audit: fix out-of-bounds read in audit_compare_dname_path() When a watch on dir=/ is combined with an fsnotify event for a single-character name directly under / (e.g., creating /a), an out-of-bounds read can occur in audit_compare_dname_path(). The helper parent_len() returns 1 for "/". In audit_compare_dname_path(), when parentlen equals the full path length (1), the code sets p = path + 1 and pathlen = 1 - 1 = 0. The subsequent loop then dereferences p[pathlen - 1] (i.e., p[-1]), causing an out-of-bounds read. Fix this by adding a pathlen > 0 check to the while loop condition to prevent the out-of-bounds access. [PM: subject tweak, sign-off email fixes]	N/A	More Details
CVE-2023-53370	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix memory leak in mes self test The fences associated with mes queue have to be freed up during amdgpu_ring_fini.	N/A	More Details
CVE-2022-50416	In the Linux kernel, the following vulnerability has been resolved: irqchip/wpcm450: Fix memory leak in wpcm450_aic_of_init() If of_iomap() failed, 'aic' should be freed before return. Otherwise there is a memory leak.	N/A	More Details
CVE-2022-50415	In the Linux kernel, the following vulnerability has been resolved: parisc: led: Fix potential null-ptr-deref in start_task() start_task() calls create_singlethread_workqueue() and not checked the ret value, which may return NULL. And a null-ptr-deref may happen: start_task() create_singlethread_workqueue() # failed, led_wq is NULL queue_delayed_work() queue_delayed_work_on() __queue_delayed_work() # warning here, but continue __queue_work() # access wq->flags, null-ptr-deref Check the ret value and return -ENOMEM if it is NULL.	N/A	More Details
CVE-2022-50414	In the Linux kernel, the following vulnerability has been resolved: scsi: fcoe: Fix transport not deattached when fcoe_if_init() fails fcoe_init() calls fcoe_transport_attach(&fcoe_sw_transport), but when fcoe_if_init() fails, &fcoe_sw_transport is not detached and leaves freed &fcoe_sw_transport on fcoe_transports list. This causes panic when reinserting module. BUG: unable to handle page fault for address: fffffbfff82e2213 RIP: 0010:fcoe_transport_attach+0xe1/0x230 [libfcoe] Call Trace: <TASK> do_one_initcall+0xd0/0x4e0 load_module+0x5eee/0x7210 ...	N/A	More Details
CVE-2022-50398	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dp: add atomic_check to bridge ops DRM commit_tails() will disable downstream crtc/encoder/bridge if both disable crtc is required and crtc->active is set before pushing a new frame downstream. There is a rare case that user space display manager issue an extra screen update immediately followed by close DRM device while down stream display interface is disabled. This extra screen update will timeout due to the downstream interface is disabled but will cause crtc->active be set. Hence the followed commit_tails() called by drm_release() will pass the disable downstream crtc/encoder/bridge conditions checking even downstream interface is disabled. This cause the crash to happen at dp_bridge_disable() due to it trying to access the main link register to push the idle pattern out while main link clocks is disabled. This patch adds atomic_check to prevent the extra frame will not be pushed down if display interface is down so that crtc->active will not be set neither. This will fail the conditions checking of disabling down stream crtc/encoder/bridge which prevent drm_release() from calling dp_bridge_disable() so that crash at dp_bridge_disable() prevented. There is no protection in the DRM framework to check if the display pipeline has been already disabled before trying again. The only check is the crtc_state->active but this is controlled by usermode using UAPI. Hence if the usermode sets this and then crashes, the driver needs to protect against double disable. SError Interrupt on CPU7, code 0x00000000be000411 -- SError CPU: 7 PID: 3878 Comm: Xorg Not tainted 5.19.0-stb-cbq #19 Hardware name: Google Lazor (rev3 - 8) (DT) pstate: a04000c9 (NzCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __cmpxchg_case_acq_32+0x14/0x2c lr : do_raw_spin_lock+0xa4/0xdc sp : ffffffc01092b6a0 x29: ffffffc01092b6a0 x28: 0000000000000028 x27: 0000000000000038 x26: 0000000000000004 x25: ffffffd2973dce48 x24: 0000000000000000 x23: 00000000ffffffff x22: 00000000ffffffff x21: ffffffd2978d0008 x20: ffffffd2978d0008 x19: ffffff80ff759fc0 x18: 0000000000000000 x17: 004800a501260460 x16: 0441043b04600438 x15: 04380000089807d0 x14: 07b0089807800780 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000438 x10: 00000000000007d0 x9 : ffffffd2973e09e4 x8 : ffffff8092d53300 x7 : ffffff808902e8b8 x6 : 0000000000000001 x5 : ffffff808902e880 x4 :	N/A	More Details

	0000000000000000 x3 : ffffff80ff759fc0 x2 : 0000000000000001 x1 : 0000000000000000 x0 : ffffff80ff759fc0 Kernel panic - not syncing: Asynchronous SError Interrupt CPU: 7 PID: 3878 Comm: Xorg Not tainted 5.19.0-stb-cbq #19 Hardware name: Google Lazor (rev3 - 8) (DT) Call trace: dump_backtrace.part.0+0xbc/0xe4 show_stack+0x24/0x70 dump_stack_lvl+0x68/0x84 dump_stack+0x18/0x34 panic+0x14c/0x32c nmi_panic+0x58/0x7c arm64_serror_panic+0x78/0x84 do_serror+0x40/0x64 el1h_64_error_handler+0x30/0x48 el1h_64_error+0x68/0x6c __cmpxchg_case_acq_32+0x14/0x2c _raw_spin_lock_irqsave+0x38/0x4c lock_timer_base+0x40/0x78 __mod_timer+0xf4/0x25c schedule_timeout+0xd4/0xfc __wait_for_common+0xac/0x140 wait_for_completion_timeout+0x2c/0x54 dp_ctrl_push_idle+0x40/0x88 dp_bridge_disable+0x24/0x30 drm_atomic_bridge_chain_disable+0x90/0xbc drm_atomic_helper_commit_modeset_disables+0x198/0x444 msm_atomic_commit_tail+0x1d0/0x374 commit_tail+0x80/0x108 drm_atomic_helper_commit+0x118/0x11c drm_atomic_commit+0xb4/0xe0 drm_client_modeset_commit_atomic+0x184/0x224 drm_client_modeset_commit_locked+0x58/0x160 drm_client_modeset_commit+0x3c/0x64 __drm_fb_helper_restore_fbdev_mode_unlocked+0x98/0xac drm_fb_helper_set_par+0x74/0x80 drm_fb_helper_hotplug_event+0xdc/0xe0 __drm_fb_helper_restore_fbdev_mode_unlocked+0x7c/0xac drm_fb_helper_restore_fbdev_mode_unlocked+0x20/0x2c drm_fb_helper_lastclose+0x20/0x2c drm_lastclose+0x44/0x6c drm_release+0x88/0xd4 __fput+0x104/0x220 ____fput+0x1c/0x28 task_work_run+0x8c/0x100 d ---truncated---		
CVE-2022-50399	In the Linux kernel, the following vulnerability has been resolved: media: atomisp: prevent integer overflow in sh_css_set_black_frame() The "height" and "width" values come from the user so the "height * width" multiplication can overflow.	N/A	More Details
CVE-2025-57440	The Blackmagic ATEM Mini Pro 2.7 exposes an undocumented Telnet service on TCP port 9993, which accepts unauthenticated plaintext commands for controlling streaming, recording, formatting storage devices, and system reboot. This interface, referred to as the "ATEM Ethernet Protocol 1.0", provides complete device control without requiring credentials or encryption. An attacker on the same network (or with remote access to the exposed port) can exploit this interface to execute arbitrary streaming commands, erase disks, or shut down the device - effectively gaining full remote control.	N/A	More Details
CVE-2022-50400	In the Linux kernel, the following vulnerability has been resolved: staging: greybus: audio_helper: remove unused and wrong debugfs usage In the greybus audio_helper code, the debugfs file for the dapm has the potential to be removed and memory will be leaked. There is also the very real potential for this code to remove ALL debugfs entries from the system, and it seems like this is what will really happen if this code ever runs. This all is very wrong as the greybus audio driver did not create this debugfs file, the sound core did and controls the lifespan of it. So remove all of the debugfs logic from the audio_helper code as there's no way it could be correct. If this really is needed, it can come back with a fixup for the incorrect usage of the debugfs_lookup() call which is what caused this to be noticed at all.	N/A	More Details
CVE-2022-50413	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix use-after-free We've already freed the assoc_data at this point, so need to use another copy of the AP (MLD) address instead.	N/A	More Details
CVE-2022-50412	In the Linux kernel, the following vulnerability has been resolved: drm: bridge: adv7511: unregister cec i2c device after cec adapter cec_unregister_adapter() assumes that the underlying adapter ops are callable. For example, if the CEC adapter currently has a valid physical address, then the unregistration procedure will invalidate the physical address by setting it to f.f.f.f. Whence the following kernel oops observed after removing the adv7511 module: Unable to handle kernel execution of user memory at virtual address 0000000000000000 Internal error: Oops: 86000004 [#1] PREEMPT_RT SMP Call trace: 0x0 adv7511_cec_adap_log_addr+0x1ac/0x1c8 [adv7511] cec_adap_unconfigure+0x44/0x90 [cec] __cec_s_phys_addr.part.0+0x68/0x230 [cec] __cec_s_phys_addr+0x40/0x50 [cec] cec_unregister_adapter+0xb4/0x118 [cec] adv7511_remove+0x60/0x90 [adv7511] i2c_device_remove+0x34/0xe0 device_release_driver_internal+0x114/0x1f0 driver_detach+0x54/0xe0 bus_remove_driver+0x60/0xd8 driver_unregister+0x34/0x60 i2c_del_driver+0x2c/0x68 adv7511_exit+0x1c/0x67c [adv7511] __arm64_sys_delete_module+0x154/0x288 invoke_syscall+0x48/0x100 el0_svc_common.constprop.0+0x48/0xe8 do_el0_svc+0x28/0x88 el0_svc+0x1c/0x50 el0t_64_sync_handler+0xa8/0xb0 el0t_64_sync+0x15c/0x160 Code: bad PC value ---[end trace 0000000000000000]--- Protect against this scenario by unregistering i2c_cec after unregistering the CEC adapter. Duly disable the CEC clock afterwards too.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: dcb: choose correct policy to parse DCB_ATTR_BCN The dcbnl_bcn_setcfg uses erroneous policy to parse tb[DCB_ATTR_BCN], which is introduced in commit 859ee3c43812 ("DCB: Add support for DCB BCN"). Please see the comment in below code static int dcbnl_bcn_setcfg(...) { ... ret = nla_parse_nested_deprecated(..., dcbnl_pfc_up_nest, ..) // !!! dcbnl_pfc_up_nest for attributes // DCB_PFC_UP_ATTR_0 to DCB_PFC_UP_ATTR_ALL in enum dcbnl_pfc_up_attrs ... for (i = DCB_BCN_ATTR_RP_0; i <= DCB_BCN_ATTR_RP_7; i++) { // !!! DCB_BCN_ATTR_RP_0 to DCB_BCN_ATTR_RP_7 in enum dcbnl_bcn_attrs ... value_byte = nla_get_u8(data[i]); ... } ... for (i = DCB_BCN_ATTR_BCNA_0; i <= DCB_BCN_ATTR_RI; i++) { // !!! DCB_BCN_ATTR_BCNA_0 to DCB_BCN_ATTR_RI in enum dcbnl_bcn_attrs ... value_int = nla_get_u32(data[i]); ... } ... } That is, the nla_parse_nested_deprecated uses dcbnl_pfc_up_nest attributes to parse nlattr defined in dcbnl_pfc_up_attrs. But the following access code fetch each nlattr as dcbnl_bcn_attrs attributes. By looking up the associated		

CVE-2023-53369	nla_policy for dcbnl_bcn_attrs. We can find the beginning part of these two policies are "same". static const struct nla_policy dcbnl_pfc_up_nest[...] = { [DCB_PFC_UP_ATTR_0] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_1] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_2] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_3] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_4] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_5] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_6] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_7] = {.type = NLA_U8}, [DCB_PFC_UP_ATTR_ALL] = {.type = NLA_FLAG}, }; static const struct nla_policy dcbnl_bcn_nest[...] = { [DCB_BCN_ATTR_RP_0] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_1] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_2] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_3] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_4] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_5] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_6] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_7] = {.type = NLA_U8}, [DCB_BCN_ATTR_RP_ALL] = {.type = NLA_FLAG}, // from here is somewhat different [DCB_BCN_ATTR_BCNA_0] = {.type = NLA_U32}, ... [DCB_BCN_ATTR_ALL] = {.type = NLA_FLAG}, }; Therefore, the current code is buggy and this nla_parse_nested_deprecated could overflow the dcbnl_pfc_up_nest and use the adjacent nla_policy to parse attributes from DCB_BCN_ATTR_BCNA_0. Hence use the correct policy dcbnl_bcn_nest to parse the nested tb[DCB_ATTR_BCN] TLV.	N/A	More Details
CVE-2023-53371	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: fix memory leak in mlx5e_fs_tt_redirect_any_create The memory pointed to by the fs->any pointer is not freed in the error path of mlx5e_fs_tt_redirect_any_create, which can lead to a memory leak. Fix by freeing the memory in the error path, thereby making the error path identical to mlx5e_fs_tt_redirect_any_destroy().	N/A	More Details
CVE-2022-50386	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix user-after-free This uses l2cap_chan_hold_unless_zero() after calling __l2cap_get_chan_blah() to prevent the following trace: Bluetooth: l2cap_core.c:static void l2cap_chan_destroy(struct kref *kref) Bluetooth: chan 0000000023c4974d Bluetooth: parent 00000000ae861c08 == BUG: KASAN: use-after-free in __mutex_waiter_is_first kernel/locking/mutex.c:191 [inline] BUG: KASAN: use-after-free in __mutex_lock_common kernel/locking/mutex.c:671 [inline] BUG: KASAN: use-after-free in __mutex_lock+0x278/0x400 kernel/locking/mutex.c:729 Read of size 8 at addr ffff888006a49b08 by task kworker/u3:2/389	N/A	More Details
CVE-2023-53372	In the Linux kernel, the following vulnerability has been resolved: sctp: fix a potential overflow in sctp_ifwdtsn_skip Currently, when traversing ifwdtsn skips with _sctp_walk_ifwdtsn, it only checks the pos against the end of the chunk. However, the data left for the last pos may be < sizeof(struct sctp_ifwdtsn_skip), and dereference it as struct sctp_ifwdtsn_skip may cause coverflow. This patch fixes it by checking the pos against "the end of the chunk - sizeof(struct sctp_ifwdtsn_skip)" in sctp_ifwdtsn_skip, similar to sctp_fwdtsn_skip.	N/A	More Details
CVE-2023-53373	In the Linux kernel, the following vulnerability has been resolved: crypto: seqiv - Handle EBUSY correctly As it is seqiv only handles the special return value of EINPROGERSS, which means that in all other cases it will free data related to the request. However, as the caller of seqiv may specify MAY_BACKLOG, we also need to expect EBUSY and treat it in the same way. Otherwise backlogged requests will trigger a use-after-free.	N/A	More Details
CVE-2022-50411	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Fix error code path in acpi_ds_call_control_method() A use-after-free in acpi_ps_parse_aml() after a failing invocaion of acpi_ds_call_control_method() is reported by KASAN [1] and code inspection reveals that next_walk_state pushed to the thread by acpi_ds_create_walk_state() is freed on errors, but it is not popped from the thread beforehand. Thus acpi_ds_get_current_walk_state() called by acpi_ps_parse_aml() subsequently returns it as the new walk state which is incorrect. To address this, make acpi_ds_call_control_method() call acpi_ds_pop_walk_state() to pop next_walk_state from the thread before returning an error.	N/A	More Details
CVE-2023-53374	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: fail SCO/ISO via hci_conn_failed if ACL gone early Not calling hci_(dis)connect_cfm before deleting conn referred to by a socket generally results to use-after-free. When cleaning up SCO connections when the parent ACL is deleted too early, use hci_conn_failed to do the connection cleanup properly. We also need to clean up ISO connections in a similar situation when connecting has started but LE Create CIS is not yet sent, so do it too here.	N/A	More Details
CVE-2022-50410	In the Linux kernel, the following vulnerability has been resolved: NFSD: Protect against send buffer overflow in NFSv2 READ Since before the git era, NFSD has conserved the number of pages held by each nfsd thread by combining the RPC receive and send buffers into a single array of pages. This works because there are no cases where an operation needs a large RPC Call message and a large RPC Reply at the same time. Once an RPC Call has been received, svc_process() updates svc_rqst::rq_res to describe the part of rq_pages that can be used for constructing the Reply. This means that the send buffer (rq_res) shrinks when the received RPC record containing the RPC Call is large. A client can force this shrinkage on TCP by sending a correctly-formed RPC Call header contained in an RPC record that is excessively large. The full maximum payload size cannot be constructed in that case.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: If sock is dead don't access sock's sk_wq in sk_stream_wait_memory Fixes the below NULL pointer dereference: [...] [14.471200] Call Trace: [14.471562] <TASK> [14.471882] lock_acquire+0x245/0x2e0 [14.472416] ? remove_wait_queue+0x12/0x50 [14.473014] ? _raw_spin_lock_irqsave+0x17/0x50 [14.473681]		

CVE-2022-50409	_raw_spin_lock_irqsave+0x3d/0x50 [14.474318] ? remove_wait_queue+0x12/0x50 [14.474907] remove_wait_queue+0x12/0x50 [14.475480] sk_stream_wait_memory+0x20d/0x340 [14.476127] ? do_wait_intr_irq+0x80/0x80 [14.476704] do_tcp_sendpages+0x287/0x600 [14.477283] tcp_bpf_push+0xab/0x260 [14.477817] tcp_bpf_sendmsg_redir+0x297/0x500 [14.478461] ? __local_bh_enable_ip+0x77/0xe0 [14.479096] tcp_bpf_send_verdict+0x105/0x470 [14.479729] tcp_bpf_sendmsg+0x318/0x4f0 [14.480311] sock_sendmsg+0x2d/0x40 [14.480822] ____sys_sendmsg+0x1b4/0x1c0 [14.481390] ? copy_msghdr_from_user+0x62/0x80 [14.482048] ___sys_sendmsg+0x78/0xb0 [14.482580] ? vmf_insert_pfn_prot+0x91/0x150 [14.483215] ? __do_fault+0x2a/0x1a0 [14.483738] ? do_fault+0x15e/0x5d0 [14.484246] ? __handle_mm_fault+0x56b/0x1040 [14.484874] ? lock_is_held_type+0xdf/0x130 [14.485474] ? find_held_lock+0x2d/0x90 [14.486046] ? __sys_sendmsg+0x41/0x70 [14.486587] __sys_sendmsg+0x41/0x70 [14.487105] ? intel_pmu_drain_pebs_core+0x350/0x350 [14.487822] do_syscall_64+0x34/0x80 [14.488345] entry_SYSCALL_64_after_hwframe+0x63/0xcd [...] The test scenario has the following flow: thread1 thread2 ---------- ---------- tcp_bpf_sendmsg tcp_bpf_send_verdict tcp_bpf_sendmsg_redir sock_close tcp_bpf_push_locked __sock_release tcp_bpf_push //inet_release do_tcp_sendpages sock->ops->release sk_stream_wait_memory // tcp_close sk_wait_event sk->sk_prot->close release_sock(__sk); *** lock_sock(sk); __tcp_close sock_orphan(sk) sk->sk_wq = NULL release_sock **** lock_sock(__sk); remove_wait_queue(sk_sleep(sk), &wait); sk_sleep(sk) //NULL pointer dereference &rcu_dereference_raw(sk->sk_wq)->wait While waiting for memory in thread1, the socket is released with its wait queue because thread2 has closed it. This caused by tcp_bpf_send_verdict didn't increase the f_count of psock->sk_redir->sk_socket->file in thread1. We should check if SOCK_DEAD flag is set on wakeup in sk_stream_wait_memory before accessing the wait queue.	N/A	More Details
CVE-2023-53375	In the Linux kernel, the following vulnerability has been resolved: tracing: Free error logs of tracing instances When a tracing instance is removed, the error messages that hold errors that occurred in the instance needs to be freed. The following reports a memory leak: # cd /sys/kernel/tracing # mkdir instances/foo # echo 'hist:keys=x' > instances/foo/events/sched/sched_switch/trigger # cat instances/foo/error_log [117.404795] hist:sched:sched_switch: error: Couldn't find field Command: hist:keys=x ^ # rmdir instances/foo Then check for memory leaks: # echo scan > /sys/kernel/debug/kmemleak # cat /sys/kernel/debug/kmemleak unreferenced object 0xffff88810d8ec700 (size 192): comm "bash", pid 869, jiffies 4294950577 (age 215.752s) hex dump (first 32 bytes): 60 dd 68 61 81 88 ff ff 60 dd 68 61 81 88 ff ff `.ha....`.ha.... a0 30 8c 83 ff ff ff ff 26 00 0a 00 00 00 00 00 .0......&..... backtrace: [<00000000dae26536>] kmalloc_trace+0x2a/0xa0 [<00000000b2938940>] tracing_log_err+0x277/0x2e0 [<000000004a0e1b07>] parse_atom+0x966/0xb40 [<0000000023b24337>] parse_expr+0x5f3/0xdb0 [<00000000594ad074>] event_hist_trigger_parse+0x27f8/0x3560 [<00000000293a9645>] trigger_process_regex+0x135/0x1a0 [<000000005c22b4f2>] event_trigger_write+0x87/0xf0 [<000000002cadc509>] vfs_write+0x162/0x670 [<0000000059c3b9be>] ksys_write+0xca/0x170 [<00000000f1cddc00>] do_syscall_64+0x3e/0xc0 [<00000000868ac68c>] entry_SYSCALL_64_after_hwframe+0x72/0xdc unreferenced object 0xffff888170c35a00 (size 32): comm "bash", pid 869, jiffies 4294950577 (age 215.752s) hex dump (first 32 bytes): 0a 20 20 43 6f 6d 6d 61 6e 64 3a 20 68 69 73 74 . Command: hist 3a 6b 65 79 73 3d 78 0a 00 00 00 00 00 00 00 00 :keys=x..... backtrace: [<000000006a747de5>] __kmalloc+0x4d/0x160 [<000000000039df5f>] tracing_log_err+0x29b/0x2e0 [<000000004a0e1b07>] parse_atom+0x966/0xb40 [<0000000023b24337>] parse_expr+0x5f3/0xdb0 [<00000000594ad074>] event_hist_trigger_parse+0x27f8/0x3560 [<00000000293a9645>] trigger_process_regex+0x135/0x1a0 [<000000005c22b4f2>] event_trigger_write+0x87/0xf0 [<000000002cadc509>] vfs_write+0x162/0x670 [<0000000059c3b9be>] ksys_write+0xca/0x170 [<00000000f1cddc00>] do_syscall_64+0x3e/0xc0 [<00000000868ac68c>] entry_SYSCALL_64_after_hwframe+0x72/0xdc The problem is that the error log needs to be freed when the instance is removed.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: fix use-after-free bug in brcmf_netdev_start_xmit() > ret = brcmf_proto_tx_queue_data(drvr, ifp->ifidx, skb); may be schedule, and then complete before the line > ndev->stats.tx_bytes += skb->len; [46.912801] == [46.920552] BUG: KASAN: use-after-free in brcmf_netdev_start_xmit+0x718/0x8c8 [brcmfmac] [46.928673] Read of size 4 at addr ffffff803f5882e8 by task systemd-resolve/328 [46.935991] [46.937514] CPU: 1 PID: 328 Comm: systemd-resolve Tainted: G O 5.4.199-[REDACTED] #1 [46.947255] Hardware name: [REDACTED] [46.954568] Call trace: [46.957037] dump_backtrace+0x0/0x2b8 [46.960719] show_stack+0x24/0x30 [46.964052] dump_stack+0x128/0x194 [46.967557] print_address_description.isra.0+0x64/0x380 [46.972877] __kasan_report+0x1d4/0x240 [46.976723] kasan_report+0xc/0x18 [46.980138] __asan_report_load4_noabort+0x18/0x20 [46.985027] brcmf_netdev_start_xmit+0x718/0x8c8 [brcmfmac] [46.990613] dev_hard_start_xmit+0x1bc/0xda0 [46.994894] sch_direct_xmit+0x198/0xd08 [46.998827] __qdisc_run+0x37c/0x1dc0 [47.002500] __dev_queue_xmit+0x1528/0x21f8 [47.006692] dev_queue_xmit+0x24/0x30 [47.010366] neigh_resolve_output+0x37c/0x678 [47.014734] ip_finish_output2+0x598/0x2458 [47.018927] __ip_finish_output+0x300/0x730 [47.023118] ip_output+0x2e0/0x430 [47.026530] ip_local_out+0x90/0x140 [47.030117] igmpv3_sendpack+0x14c/0x228 [47.034049] igmpv3_send_cr+0x384/0x6b8 [47.037895] igmp_ifc_timer_expire+0x4c/0x118 [47.042262] call_timer_fn+0x1cc/0xbe8 [47.046021] __run_timers+0x4d8/0xb28 [47.049693] run_timer_softirq+0x24/0x40 [47.053626] __do_softirq+0x2c0/0x117c [47.057387] irq_exit+0x2dc/0x388 [47.060715] __handle_domain_irq+0xb4/0x158 [47.064908] gic_handle_irq+0x58/0xb0 [47.068581]		More

2022-50408	el0_irq_naked+0x50/0x5c [47.072162] [47.073665] Allocated by task 328: [47.077083] save_stack+0x24/0xb0 [47.080410] __kasan_kmalloc.isra.0+0xc0/0xe0 [47.084776] kasan_slab_alloc+0x14/0x20 [47.088622] kmem_cache_alloc+0x15c/0x468 [47.092643] __alloc_skb+0xa4/0x498 [47.096142] igmpv3_newpack+0x158/0xd78 [47.099987] add_grhead+0x210/0x288 [47.103485] add_grec+0x6b0/0xb70 [47.106811] igmpv3_send_cr+0x2e0/0x6b8 [47.110657] igmp_ifc_timer_expire+0x4c/0x118 [47.115027] call_timer_fn+0x1cc/0xbe8 [47.118785] __run_timers+0x4d8/0xb28 [47.122457] run_timer_softirq+0x24/0x40 [47.126389] __do_softirq+0x2c0/0x117c [47.130142] [47.131643] Freed by task 180: [47.134712] save_stack+0x24/0xb0 [47.138041] __kasan_slab_free+0x108/0x180 [47.142146] kasan_slab_free+0x10/0x18 [47.145904] slab_free_freelist_hook+0xa4/0x1b0 [47.150444] kmem_cache_free+0x8c/0x528 [47.154292] kfree_skbmem+0x94/0x108 [47.157880] consume_skb+0x10c/0x5a8 [47.161466] __dev_kfree_skb_any+0x88/0xa0 [47.165598] brcmu_pkt_buf_free_skb+0x44/0x68 [brcmutil] [47.171023] brcmf_txfinalize+0xec/0x190 [brcmfmac] [47.176016] brcmf_proto_bcdc_txcomplete+0x1c0/0x210 [brcmfmac] [47.182056] brcmf_sdio_sendfromq+0x8dc/0x1e80 [brcmfmac] [47.187568] brcmf_sdio_dpc+0xb48/0x2108 [brcmfmac] [47.192529] brcmf_sdio_dataworker+0xc8/0x238 [brcmfmac] [47.197859] process_one_work+0x7fc/0x1a80 [47.201965] worker_thread+0x31c/0xc40 [47.205726] kthread+0x2d8/0x370 [47.208967] ret_from_fork+0x10/0x18 [47.212546] [47.214051] The buggy address belongs to the object at ffffff803f588280 [47.214051] which belongs to the cache skbuff_head_cache of size 208 [47.227086] The buggy address is located 104 bytes inside of [47.227086] 208-byte region [ffffff803f588280, ffffff803f588350) [47.238814] The buggy address belongs to the page: [47.243618] page:ffffffff00dd6200 refcount:1 mapcou ---truncated---	N/A	Details
CVE-2022-50407	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/qm - increase the memory of local variables Increase the buffer to prevent stack overflow by fuzz test. The maximum length of the qos configuration buffer is 256 bytes. Currently, the value of the 'val buffer' is only 32 bytes. The sscanf does not check the dest memory length. So the 'val buffer' may stack overflow.	N/A	More Details
CVE-2022-50406	In the Linux kernel, the following vulnerability has been resolved: iomap: iomap: fix memory corruption when recording errors during writeback Every now and then I see this crash on arm64: Unable to handle kernel NULL pointer dereference at virtual address 00000000000000f8 Buffer I/O error on dev dm-0, logical block 8733687, async page read Mem abort info: ESR = 0x0000000096000006 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault Data abort info: ISV = 0, ISS = 0x00000006 CM = 0, WnR = 0 user pgtable: 64k pages, 42-bit VAs, pgdp=0000000139750000 [00000000000000f8] pgd=0000000000000000, p4d=0000000000000000, pud=0000000000000000, pmd=0000000000000000 Internal error: Oops: 96000006 [#1] PREEMPT SMP Buffer I/O error on dev dm-0, logical block 8733688, async page read Dumping ftrace buffer: Buffer I/O error on dev dm-0, logical block 8733689, async page read (ftrace buffer empty) XFS (dm-0): log I/O error -5 Modules linked in: dm_thin_pool dm_persistent_data XFS (dm-0): Metadata I/O Error (0x1) detected at xfs_trans_read_buf_map+0x1ec/0x590 [xfs] (fs/xfs/xfs_trans_buf.c:296). dm_bio_prison XFS (dm-0): Please unmount the filesystem and rectify the problem(s) XFS (dm-0): xfs_imap_lookup: xfs_ialloc_read_agi() returned error -5, agno 0 dm_bufio dm_log_writes xfs nft_chain_nat xt_REDIRECT nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip6t_REJECT potentially unexpected fatal signal 6. nf_reject_ipv6 potentially unexpected fatal signal 6. ipt_REJECT nf_reject_ipv4 CPU: 1 PID: 122166 Comm: fsstress Tainted: G W 6.0.0-rc5-djwa #rc5 3004c9f1de887ebae86015f2677638ce51ee7 rpcsec_gss_krb5 auth_rpcgss xt_tcpudp ip_set_hash_ip ip_set_hash_net xt_set nft_compat ip_set_hash_mac ip_set nf_tables Hardware name: QEMU KVM Virtual Machine, BIOS 1.5.1 06/16/2021 pstate: 60001000 (nZCv daif -PAN -UAO -TCO -DIT +SSBS BTYPE=--) ip_tables pc : 000003fd6d7df200 x_tables lr : 000003fd6d7df1ec overlay nfsv4 CPU: 0 PID: 54031 Comm: u4:3 Tainted: G W 6.0.0-rc5-djwa #rc5 3004c9f1de887ebae86015f2677638ce51ee7405 Hardware name: QEMU KVM Virtual Machine, BIOS 1.5.1 06/16/2021 Workqueue: writeback wb_workfn sp : 000003ffd9522fd0 (flush-253:0) pstate: 60401005 (nZCv daif +PAN -UAO -TCO -DIT +SSBS BTYPE=--) pc : errseq_set+0x1c/0x100 x29: 000003ffd9522fd0 x28: 0000000000000023 x27: 000002acefeb6780 x26: 0000000000000005 x25: 0000000000000001 x24: 0000000000000000 x23: 00000000ffffffff x22: 0000000000000005 lr : __filemap_set_wb_err+0x24/0xe0 x21: 0000000000000006 sp : fffffe000f80f760 x29: fffffe000f80f760 x28: 0000000000000003 x27: fffffe000f80f9f8 x26: 0000000002523000 x25: 00000000fffffffb x24: fffffe000f80f868 x23: fffffe000f80fbb0 x22: fffffc0180c26a78 x21: 0000000002530000 x20: 0000000000000000 x19: 0000000000000000 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000001 x13: 0000000000470af3 x12: fffffc0058f70000 x11: 0000000000000040 x10: 0000000000001b20 x9 : fffffe000836b288 x8 : fffffc00eb9fd480 x7 : 0000000000f83659 x6 : 0000000000000000 x5 : 0000000000000869 x4 : 0000000000000005 x3 : 00000000000000f8 x20: 000003fd6d740020 x19: 000000000001dd36 x18: 0000000000000001 x17: 000003fd6d78704c x16: 0000000000000001 x15: 000002acfac87668 x2 : 0000000000000ffa x1 : 00000000ffffffff x0 : 00000000000000f8 Call trace: errseq_set+0x1c/0x100 __filemap_set_wb_err+0x24/0xe0 iomap_do_writepage+0x5e4/0xd5c write_cache_pages+0x208/0x674 iomap_writepages+0x34/0x60 xfs_vm_writepages+0x8c/0xcc [xfs 7a861f39c43631f15d3a5884246ba5035d4ca78b] x14: 0000000000000000 x13: 2064656e72757465 x12: 0000000000002180 x11: 000003fd6d8a82d0 x10: 0000000000000000 x9 : 000003fd6d8ae288 x8 : 0000000000000083 x7 : 00000000ffffffff x6 : 00000000ffffffee x5 : 00000000fbad2887 x4 : 000003fd6d9abb58 x3 : 000003fd6d740020 x2 : 0000000000000006 x1 : 000000000001dd36 x0 : 0000000000000000 CPU: ---truncated---	N/A	More Details

CVE-2022-50397	In the Linux kernel, the following vulnerability has been resolved: net/ieee802154: reject zero-sized raw_sendmsg() syzbot is hitting skb_assert_len() warning at raw_sendmsg() for ieee802154 socket. What commit dc633700f00f726e ("net/af_packet: check len when min_header_len equals to 0") does also applies to ieee802154 socket.	N/A	More Details
CVE-2025-55886	An Insecure Direct Object Reference (IDOR) vulnerability was discovered in ARD. The flaw exists in the `fe_uid` parameter of the payment history API endpoint. An authenticated attacker can manipulate this parameter to access the payment history of other users without authorization.	N/A	More Details
CVE-2022-50417	In the Linux kernel, the following vulnerability has been resolved: drm/panfrost: Fix GEM handle creation ref-counting panfrost_gem_create_with_handle() previously returned a BO but with the only reference being from the handle, which user space could in theory guess and release, causing a use-after-free. Additionally if the call to panfrost_gem_mapping_get() in panfrost_ioctl_create_bo() failed then a(nother) reference on the BO was dropped. The _create_with_handle() is a problematic pattern, so ditch it and instead create the handle in panfrost_ioctl_create_bo(). If the call to panfrost_gem_mapping_get() fails then this means that user space has indeed gone behind our back and freed the handle. In which case just return an error code.	N/A	More Details
CVE-2022-50396	In the Linux kernel, the following vulnerability has been resolved: net: sched: fix memory leak in tcindex_set_parms Syzkaller reports a memory leak as follows: ========== BUG: memory leak unreferenced object 0xffff88810c287f00 (size 256): comm "syz-executor105", pid 3600, jiffies 4294943292 (age 12.990s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<ffffffff814cf9f0>] kmalloc_trace+0x20/0x90 mm/slab_common.c:1046 [<ffffffff839c9e07>] kmalloc include/linux/slab.h:576 [inline] [<ffffffff839c9e07>] kmalloc_array include/linux/slab.h:627 [inline] [<ffffffff839c9e07>] kcalloc include/linux/slab.h:659 [inline] [<ffffffff839c9e07>] tcf_exts_init include/net/pkt_cls.h:250 [inline] [<ffffffff839c9e07>] tcindex_set_parms+0xa7/0xbe0 net/sched/cls_tcindex.c:342 [<ffffffff839caa1f>] tcindex_change+0xdf/0x120 net/sched/cls_tcindex.c:553 [<ffffffff8394db62>] tc_new_tfilter+0x4f2/0x1100 net/sched/cls_api.c:2147 [<ffffffff8389e91c>] rtnetlink_rcv_msg+0x4dc/0x5d0 net/core/rtnetlink.c:6082 [<ffffffff839eba67>] netlink_rcv_skb+0x87/0x1d0 net/netlink/af_netlink.c:2540 [<ffffffff839eab87>] netlink_unicast_kernel net/netlink/af_netlink.c:1319 [inline] [<ffffffff839eab87>] netlink_unicast+0x397/0x4c0 net/netlink/af_netlink.c:1345 [<ffffffff839eb046>] netlink_sendmsg+0x396/0x710 net/netlink/af_netlink.c:1921 [<ffffffff8383e796>] sock_sendmsg_nosec net/socket.c:714 [inline] [<ffffffff8383e796>] sock_sendmsg+0x56/0x80 net/socket.c:734 [<ffffffff8383eb08>] ___sys_sendmsg+0x178/0x410 net/socket.c:2482 [<ffffffff83843678>] ___sys_sendmsg+0xa8/0x110 net/socket.c:2536 [<ffffffff838439c5>] __sys_sendmmsg+0x105/0x330 net/socket.c:2622 [<ffffffff83843c14>] __do_sys_sendmmsg net/socket.c:2651 [inline] [<ffffffff83843c14>] __se_sys_sendmmsg net/socket.c:2648 [inline] [<ffffffff83843c14>] __x64_sys_sendmmsg+0x24/0x30 net/socket.c:2648 [<ffffffff84605fd5>] do_syscall_x64 arch/x86/entry/common.c:50 [inline] [<ffffffff84605fd5>] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 [<ffffffff84800087>] entry_SYSCALL_64_after_hwframe+0x63/0xcd ========== Kernel uses tcindex_change() to change an existing filter properties. Yet the problem is that, during the process of changing, if `old_r` is retrieved from `p->perfect`, then kernel uses tcindex_alloc_perfect_hash() to newly allocate filter results, uses tcindex_filter_result_init() to clear the old filter result, without destroying its tcf_exts structure, which triggers the above memory leak. To be more specific, there are only two source for the `old_r`, according to the tcindex_lookup(). `old_r` is retrieved from `p->perfect`, or `old_r` is retrieved from `p->h`. * If `old_r` is retrieved from `p->perfect`, kernel uses tcindex_alloc_perfect_hash() to newly allocate the filter results. Then `r` is assigned with `cp->perfect + handle`, which is newly allocated. So condition `old_r && old_r != r` is true in this situation, and kernel uses tcindex_filter_result_init() to clear the old filter result, without destroying its tcf_exts structure * If `old_r` is retrieved from `p->h`, then `p->perfect` is NULL according to the tcindex_lookup(). Considering that `cp->h` is directly copied from `p->h` and `p->perfect` is NULL, `r` is assigned with `tcindex_lookup(cp, handle)`, whose value should be the same as `old_r`, so condition `old_r && old_r != r` is false in this situation, kernel ignores using tcindex_filter_result_init() to clear the old filter result. So only when `old_r` is retrieved from `p->perfect` does kernel use tcindex_filter_result_init() to clear the old filter result, which triggers the above memory leak. Considering that there already exists a tc_filter_wq workqueue to destroy the old tcindex_d ---truncated---	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nvme: fix multipath crash caused by flush request when blktrace is enabled The flush request initialized by blk_kick_flush has NULL bio, and it may be dealt with nvme_end_req during io completion. When blktrace is enabled, nvme_trace_bio_complete with multipath activated trying to access NULL pointer bio from flush request results in the following crash: [2517.831677] BUG: kernel NULL pointer dereference, address: 000000000000001a [2517.835213] #PF: supervisor read access in kernel mode [2517.838724] #PF: error_code(0x0000) - not-present page [2517.842222] PGD 7b2d51067 P4D 0 [2517.845684] Oops: 0000 [#1] SMP NOPTI [2517.849125] CPU: 2 PID: 732 Comm: kworker/2:1H Kdump: loaded Tainted: G S 5.15.67-0.cl9.x86_64 #1 [2517.852723] Hardware name: XFUSION 2288H V6/BC13MBSBC, BIOS 1.13 07/27/2022 [2517.856358] Workqueue: nvme_tcp_wq nvme_tcp_io_work [nvme_tcp] [2517.859993] RIP: 0010:blk_add_trace_bio_complete+0x6/0x30 [2517.863628] Code: 1f 44 00 00 48 8b 46 08 31 c9 ba 04 00 10 00 48 8b 80 50 03 00 00 48 8b 78 50 e9 e5 fe ff ff 0f 1f 44 00 00 41 54 49 89 f4 55 <0f> b6 7a 1a 48 89		

CVE-2022-50388	d5 e8 3e 1c 2b 00 48 89 ee 4c 89 e7 5d 89 c1 ba [2517.871269] RSP: 0018:ff7f6a008d9dbcd0 EFLAGS: 00010286 [2517.875081] RAX: ff3d5b4be00b1d50 RBX: 0000000002040002 RCX: ff3d5b0a270f2000 [2517.878966] RDX: 0000000000000000 RSI: ff3d5b0b021fb9f8 RDI: 0000000000000000 [2517.882849] RBP: ff3d5b0b96a6fa00 R08: 0000000000000001 R09: 0000000000000000 [2517.886718] R10: 000000000000000c R11: 000000000000000c R12: ff3d5b0b021fb9f8 [2517.890575] R13: 0000000002000000 R14: ff3d5b0b021fb1b0 R15: 0000000000000018 [2517.894434] FS: 0000000000000000(0000) GS:ff3d5b42bfc80000(0000) knlGS:0000000000000000 [2517.898299] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [2517.902157] CR2: 000000000000001a CR3: 00000004f023e005 CR4: 0000000000771ee0 [2517.906053] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [2517.909930] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [2517.913761] PKRU: 55555554 [2517.917558] Call Trace: [2517.921294] <TASK> [2517.924982] nvme_complete_rq+0x1c3/0x1e0 [nvme_core] [2517.928715] nvme_tcp_recv_pdu+0x4d7/0x540 [nvme_tcp] [2517.932442] nvme_tcp_recv_skb+0x4f/0x240 [nvme_tcp] [2517.936137] ? nvme_tcp_recv_pdu+0x540/0x540 [nvme_tcp] [2517.939830] tcp_read_sock+0x9c/0x260 [2517.943486] nvme_tcp_try_recv+0x65/0xa0 [nvme_tcp] [2517.947173] nvme_tcp_io_work+0x64/0x90 [nvme_tcp] [2517.950834] process_one_work+0x1e8/0x390 [2517.954473] worker_thread+0x53/0x3c0 [2517.958069] ? process_one_work+0x390/0x390 [2517.961655] kthread+0x10c/0x130 [2517.965211] ? set_kthread_struct+0x40/0x40 [2517.968760] ret_from_fork+0x1f/0x30 [2517.972285] </TASK> To avoid this situation, add a NULL check for req->bio before calling trace_block_bio_complete.	N/A	More Details
CVE-2023-53427	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix warning and UAF when destroy the MR list If the MR allocate failed, the MR recovery work not initialized and list not cleared. Then will be warning and UAF when release the MR: WARNING: CPU: 4 PID: 824 at kernel/workqueue.c:3066 __flush_work.isra.0+0xf7/0x110 CPU: 4 PID: 824 Comm: mount.cifs Not tainted 6.1.0-rc5+ #82 RIP: 0010:__flush_work.isra.0+0xf7/0x110 Call Trace: <TASK> __cancel_work_timer+0x2ba/0x2e0 smbd_destroy+0x4e1/0x990 _smbd_get_connection+0x1cbd/0x2110 smbd_get_connection+0x21/0x40 cifs_get_tcp_session+0x8ef/0xda0 mount_get_conns+0x60/0x750 cifs_mount+0x103/0xd00 cifs_smb3_do_mount+0x1dd/0xcb0 smb3_get_tree+0x1d5/0x300 vfs_get_tree+0x41/0xf0 path_mount+0x9b3/0xdd0 __x64_sys_mount+0x190/0x1d0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 BUG: KASAN: use-after-free in smbd_destroy+0x4fc/0x990 Read of size 8 at addr ffff88810b156a08 by task mount.cifs/824 CPU: 4 PID: 824 Comm: mount.cifs Tainted: G W 6.1.0-rc5+ #82 Call Trace: dump_stack_lvl+0x34/0x44 print_report+0x171/0x472 kasan_report+0xad/0x130 smbd_destroy+0x4fc/0x990 _smbd_get_connection+0x1cbd/0x2110 smbd_get_connection+0x21/0x40 cifs_get_tcp_session+0x8ef/0xda0 mount_get_conns+0x60/0x750 cifs_mount+0x103/0xd00 cifs_smb3_do_mount+0x1dd/0xcb0 smb3_get_tree+0x1d5/0x300 vfs_get_tree+0x41/0xf0 path_mount+0x9b3/0xdd0 __x64_sys_mount+0x190/0x1d0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 Allocated by task 824: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 __kasan_kmalloc+0x7a/0x90 _smbd_get_connection+0x1b6f/0x2110 smbd_get_connection+0x21/0x40 cifs_get_tcp_session+0x8ef/0xda0 mount_get_conns+0x60/0x750 cifs_mount+0x103/0xd00 cifs_smb3_do_mount+0x1dd/0xcb0 smb3_get_tree+0x1d5/0x300 vfs_get_tree+0x41/0xf0 path_mount+0x9b3/0xdd0 __x64_sys_mount+0x190/0x1d0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 Freed by task 824: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 kasan_save_free_info+0x2a/0x40 ____kasan_slab_free+0x143/0x1b0 __kmem_cache_free+0xc8/0x330 _smbd_get_connection+0x1c6a/0x2110 smbd_get_connection+0x21/0x40 cifs_get_tcp_session+0x8ef/0xda0 mount_get_conns+0x60/0x750 cifs_mount+0x103/0xd00 cifs_smb3_do_mount+0x1dd/0xcb0 smb3_get_tree+0x1d5/0x300 vfs_get_tree+0x41/0xf0 path_mount+0x9b3/0xdd0 __x64_sys_mount+0x190/0x1d0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 Let's initialize the MR recovery work before MR allocate to prevent the warning, remove the MRs from the list to prevent the UAF.	N/A	More Details
CVE-2023-53426	In the Linux kernel, the following vulnerability has been resolved: xsk: Fix xsk_diag use-after-free error during socket cleanup Fix a use-after-free error that is possible if the xsk_diag interface is used after the socket has been unbound from the device. This can happen either due to the socket being closed or the device disappearing. In the early days of AF_XDP, the way we tested that a socket was not bound to a device was to simply check if the netdevice pointer in the xsk socket structure was NULL. Later, a better system was introduced by having an explicit state variable in the xsk socket struct. For example, the state of a socket that is on the way to being closed and has been unbound from the device is XSK_UNBOUND. The commit in the Fixes tag below deleted the old way of signalling that a socket is unbound, setting dev to NULL. This in the belief that all code using the old way had been exterminated. That was unfortunately not true as the xsk diagnostics code was still using the old way and thus does not work as intended when a socket is going down. Fix this by introducing a test against the state variable. If the socket is in the state XSK_UNBOUND, simply abort the diagnostic's netlink operation.	N/A	More Details
CVE-2023-53425	In the Linux kernel, the following vulnerability has been resolved: media: platform: mediatek: vpu: fix NULL ptr dereference If pdev is NULL, then it is still dereferenced. This fixes this smatch warning: drivers/media/platform/mediatek/vpu/mtk_vpu.c:570 vpu_load_firmware() warn: address of NULL pointer 'pdev'	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: tpm: tpm_crb: Add the missed		

2022-50389	acpi_put_table() to fix memory leak In crb_acpi_add(), we get the TPM2 table to retrieve information like start method, and then assign them to the priv data, so the TPM2 table is not used after the init, should be freed, call acpi_put_table() to fix the memory leak.	N/A	More Details
CVE-2023-53424	In the Linux kernel, the following vulnerability has been resolved: clk: mediatek: fix of_iomap memory leak Smatch reports: drivers/clk/mediatek/clk-mtk.c:583 mtk_clk_simple_probe() warn: 'base' from of_iomap() not released on lines: 496. This problem was also found in linux-next. In mtk_clk_simple_probe(), base is not released when handling errors if clk_data is not existed, which may cause a leak. So free_base should be added here to release base.	N/A	More Details
CVE-2022-50390	In the Linux kernel, the following vulnerability has been resolved: drm/ttm: fix undefined behavior in bit shift for TTM_TT_FLAG_PRIV_POPULATED Shifting signed 32-bit value by 31 bits is undefined, so changing significant bit to unsigned. The UBSAN warning calltrace like below: UBSAN: shift-out-of-bounds in ./include/drm/ttm/ttm_tt.h:122:26 left shift of 1 by 31 places cannot be represented in type 'int' Call Trace: <TASK> dump_stack_lvl+0x7d/0xa5 dump_stack+0x15/0x1b ubsan_epilogue+0xe/0x4e __ubsan_handle_shift_out_of_bounds+0x1e7/0x20c ttm_bo_move_memcpy+0x3b4/0x460 [ttm] bo_driver_move+0x32/0x40 [drm_vram_helper] ttm_bo_handle_move_mem+0x118/0x200 [ttm] ttm_bo_validate+0xfa/0x220 [ttm] drm_gem_vram_pin_locked+0x70/0x1b0 [drm_vram_helper] drm_gem_vram_pin+0x48/0xb0 [drm_vram_helper] drm_gem_vram_plane_helper_prepare_fb+0x53/0xe0 [drm_vram_helper] drm_gem_vram_simple_display_pipe_prepare_fb+0x26/0x30 [drm_vram_helper] drm_simple_kms_plane_prepare_fb+0x4d/0xe0 [drm_kms_helper] drm_atomic_helper_prepare_planes+0xda/0x210 [drm_kms_helper] drm_atomic_helper_commit+0xc3/0x1e0 [drm_kms_helper] drm_atomic_commit+0x9c/0x160 [drm] drm_client_modeset_commit_atomic+0x33a/0x380 [drm] drm_client_modeset_commit_locked+0x77/0x220 [drm] drm_client_modeset_commit+0x31/0x60 [drm] __drm_fb_helper_restore_fbdev_mode_unlocked+0xa7/0x170 [drm_kms_helper] drm_fb_helper_set_par+0x51/0x90 [drm_kms_helper] fbcon_init+0x316/0x790 visual_init+0x113/0x1d0 do_bind_con_driver+0x2a3/0x5c0 do_take_over_console+0xa9/0x270 do_fbcon_takeover+0xa1/0x170 do_fb_registered+0x2a8/0x340 fbcon_fb_registered+0x47/0xe0 register_framebuffer+0x294/0x4a0 __drm_fb_helper_initial_config_and_unlock+0x43c/0x880 [drm_kms_helper] drm_fb_helper_initial_config+0x52/0x80 [drm_kms_helper] drm_fbdev_client_hotplug+0x156/0x1b0 [drm_kms_helper] drm_fbdev_generic_setup+0xfc/0x290 [drm_kms_helper] bochs_pci_probe+0x6ca/0x772 [bochs] local_pci_probe+0x4d/0xb0 pci_device_probe+0x119/0x320 really_probe+0x181/0x550 __driver_probe_device+0xc6/0x220 driver_probe_device+0x32/0x100 __driver_attach+0x195/0x200 bus_for_each_dev+0xbb/0x120 driver_attach+0x27/0x30 bus_add_driver+0x22e/0x2f0 driver_register+0xa9/0x190 __pci_register_driver+0x90/0xa0 bochs_pci_driver_init+0x52/0x1000 [bochs] do_one_initcall+0x76/0x430 do_init_module+0x61/0x28a load_module+0x1f82/0x2e50 __do_sys_finit_module+0xf8/0x190 __x64_sys_finit_module+0x23/0x30 do_syscall_64+0x58/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd </TASK>	N/A	More Details
CVE-2025-39849	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: sme: cap SSID length in __cfg80211_connect_result() If the ssid->datalen is more than IEEE80211_MAX_SSID_LEN (32) it would lead to memory corruption so add some bounds checking.	N/A	More Details
CVE-2025-43807	Stored cross-site scripting (XSS) vulnerability in the notifications widget in Liferay Portal 7.4.0 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a publication’s “Name” text field.	N/A	More Details
CVE-2022-50391	In the Linux kernel, the following vulnerability has been resolved: mm/mempolicy: fix memory leak in set_mempolicy_home_node system call When encountering any vma in the range with policy other than MPOL_BIND or MPOL_PREFERRED_MANY, an error is returned without issuing a mpol_put on the policy just allocated with mpol_dup(). This allows arbitrary users to leak kernel memory.	N/A	More Details
CVE-2023-53423	In the Linux kernel, the following vulnerability has been resolved: objtool: Fix memory leak in create_static_call_sections() strdup() allocates memory for key_name. We need to release the memory in the following error paths. Add free() to avoid memory leak.	N/A	More Details
CVE-2023-53422	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: fw: fix memory leak in debugfs Fix a memory leak that occurs when reading the fw_info file all the way, since we return NULL indicating no more data, but don't free the status tracking object.	N/A	More Details
CVE-2023-53421	In the Linux kernel, the following vulnerability has been resolved: blk-cgroup: Reinit blkg_iostat_set after clearing in blkcg_reset_stats() When blkg_alloc() is called to allocate a blkcg_gq structure with the associated blkg_iostat_set's, there are 2 fields within blkg_iostat_set that requires proper initialization - blkg & sync. The former field was introduced by commit 3b8cc6298724 ("blk-cgroup: Optimize blkcg_rstat_flush()") while the later one was introduced by commit f73316482977 ("blk-cgroup: reimplement basic IO stats using cgroup rstat"). Unfortunately those fields in the blkg_iostat_set's are not properly re-initialized when they are cleared in v1's blkcg_reset_stats(). This can lead to a kernel panic due to NULL pointer access of the blkg pointer. The missing initialization of sync is less problematic and can be a problem in a debug kernel due to missing lockdep initialization. Fix these problems by re-initializing them after memory clearing.	N/A	More Details

CVE-2023-53420	In the Linux kernel, the following vulnerability has been resolved: ntfs: Fix panic about slab-out-of-bounds caused by ntfs_listxattr() Here is a BUG report from syzbot: BUG: KASAN: slab-out-of-bounds in ntfs_list_ea fs/ntfs3/xattr.c:191 [inline] BUG: KASAN: slab-out-of-bounds in ntfs_listxattr+0x401/0x570 fs/ntfs3/xattr.c:710 Read of size 1 at addr ffff888021acaf3d by task syz-executor128/3632 Call Trace: ntfs_list_ea fs/ntfs3/xattr.c:191 [inline] ntfs_listxattr+0x401/0x570 fs/ntfs3/xattr.c:710 vfs_listxattr fs/xattr.c:457 [inline] listxattr+0x293/0x2d0 fs/xattr.c:804 Fix the logic of ea_all iteration. When the ea->name_len is 0, return immediately, or Add2Ptr() would visit invalid memory in the next loop. [almaz.alexandrovich@paragon-software.com: lines of the patch have changed]	N/A	More Details
CVE-2023-53419	In the Linux kernel, the following vulnerability has been resolved: rcu: Protect rcu_print_task_exp_stall() ->exp_tasks access For kernels built with CONFIG_PREEMPT_RCU=y, the following scenario can result in a NULL-pointer dereference: CPU1 CPU2 rcu_preempt_deferred_qs_irqrestore rcu_print_task_exp_stall if (special.b.blocked) READ_ONCE(rnp->exp_tasks) != NULL raw_spin_lock_rcu_node np = rcu_next_node_entry(t, rnp) if (&t->rcu_node_entry == rnp->exp_tasks) WRITE_ONCE(rnp->exp_tasks, np) .... raw_spin_unlock_irqrestore_rcu_node raw_spin_lock_irqsave_rcu_node t = list_entry(rnp->exp_tasks->prev, struct task_struct, rcu_node_entry) (if rnp->exp_tasks is NULL, this will dereference a NULL pointer) The problem is that CPU2 accesses the rcu_node structure's->exp_tasks field without holding the rcu_node structure's ->lock and CPU2 did not observe CPU1's change to rcu_node structure's ->exp_tasks in time. Therefore, if CPU1 sets rcu_node structure's->exp_tasks pointer to NULL, then CPU2 might dereference that NULL pointer. This commit therefore holds the rcu_node structure's ->lock while accessing that structure's->exp_tasks field. [paulmck: Apply Frederic Weisbecker feedback.]	N/A	More Details
CVE-2022-50392	In the Linux kernel, the following vulnerability has been resolved: ASoC: mediatek: mt8183: fix refcount leak in mt8183_mt6358_ts3a227_max98357_dev_probe() The node returned by of_parse_phandle() with refcount incremented, of_node_put() needs be called when finish using it. So add it in the error path in mt8183_mt6358_ts3a227_max98357_dev_probe().	N/A	More Details
CVE-2022-50393	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: SDMA update use unlocked iterator SDMA update page table may be called from unlocked context, this generate below warning. Use unlocked iterator to handle this case. WARNING: CPU: 0 PID: 1475 at drivers/dma-buf/dma-resv.c:483 dma_resv_iter_next Call Trace: dma_resv_iter_first+0x43/0xa0 amdgpu_vm_sdma_update+0x69/0x2d0 [amdgpu] amdgpu_vm_ptes_update+0x29c/0x870 [amdgpu] amdgpu_vm_update_range+0x2f6/0x6c0 [amdgpu] svm_range_unmap_from_gpus+0x115/0x300 [amdgpu] svm_range_cpu_invalidate_pagetables+0x510/0x5e0 [amdgpu] __mmu_notifier_invalidate_range_start+0x1d3/0x230 unmap_vmas+0x140/0x150 unmap_region+0xa8/0x110	N/A	More Details
CVE-2022-50419	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sysfs: Fix attempting to call device_add multiple times device_add shall not be called multiple times as stated in its documentation: 'Do not call this routine or device_register() more than once for any device structure' Syzkaller reports a bug as follows [1]: ------------[cut here]------------ kernel BUG at lib/list_debug.c:33! invalid opcode: 0000 [#1] PREEMPT SMP KASAN [...] Call Trace: <TASK> __list_add include/linux/list.h:69 [inline] list_add_tail include/linux/list.h:102 [inline] kobj_kset_join lib/kobject.c:164 [inline] kobject_add_internal+0x18f/0x8f0 lib/kobject.c:214 kobject_add_varg lib/kobject.c:358 [inline] kobject_add+0x150/0x1c0 lib/kobject.c:410 device_add+0x368/0x1e90 drivers/base/core.c:3452 hci_conn_add_sysfs+0x9b/0x1b0 net/bluetooth/hci_sysfs.c:53 hci_le_cis_estabilished_evt+0x57c/0xae0 net/bluetooth/hci_event.c:6799 hci_le_meta_evt+0x2b8/0x510 net/bluetooth/hci_event.c:7110 hci_event_func net/bluetooth/hci_event.c:7440 [inline] hci_event_packet+0x63d/0xfd0 net/bluetooth/hci_event.c:7495 hci_rx_work+0xae7/0x1230 net/bluetooth/hci_core.c:4007 process_one_work+0x991/0x1610 kernel/workqueue.c:2289 worker_thread+0x665/0x1080 kernel/workqueue.c:2436 kthread+0x2e4/0x3a0 kernel/kthread.c:376 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:306 </TASK>	N/A	More Details
CVE-2022-50394	In the Linux kernel, the following vulnerability has been resolved: i2c: ismt: Fix an out-of-bounds bug in ismt_access() When the driver does not check the data from the user, the variable 'data->block[0]' may be very large to cause an out-of-bounds bug. The following log can reveal it: [33.995542] i2c i2c-1: ioctl, cmd=0x720, arg=0x7ffcb3dc3a20 [33.995978] ismt_smbus 0000:00:05.0: I2C_SMBUS_BLOCK_DATA: WRITE [33.996475] == [33.996995] BUG: KASAN: out-of-bounds in ismt_access.cold+0x374/0x214b [33.997473] Read of size 18446744073709551615 at addr ffff88810efcfdb1 by task ismt_poc/485 [33.999450] Call Trace: [34.001849] memcpy+0x20/0x60 [34.002077] ismt_access.cold+0x374/0x214b [34.003382] __i2c_smbus_xfer+0x44f/0xfb0 [34.004007] i2c_smbus_xfer+0x10a/0x390 [34.004291] i2cdev_ioctl_smbus+0x2c8/0x710 [34.005196] i2cdev_ioctl+0x5ec/0x74c Fix this bug by checking the size of 'data->block[0]' first.	N/A	More Details
CVE-2022-50395	In the Linux kernel, the following vulnerability has been resolved: integrity: Fix memory leakage in keyring allocation error path Key restriction is allocated in integrity_init_keyring(). However, if keyring allocation failed, it is not freed, causing memory leaks.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: mhi: fix potential memory leak in ath11k_mhi_register() mhi_alloc_controller() allocates a memory space for mhi_ctrl. When gets some error,		

2022-50418	mhi_ctrl should be freed with mhi_free_controller(). But when ath11k_mhi_read_addr_from_dt() fails, the function returns without calling mhi_free_controller(), which will lead to a memory leak. We can fix it by calling mhi_free_controller() when ath11k_mhi_read_addr_from_dt() fails.	N/A	More Details
CVE-2022-50405	In the Linux kernel, the following vulnerability has been resolved: net/tunnel: wait until all sk_user_data reader finish before releasing the sock There is a race condition in vxlan that when deleting a vxlan device during receiving packets, there is a possibility that the sock is released after getting vxlan_sock vs from sk_user_data. Then in later vxlan_ecn_decapsulate(), vxlan_get_sk_family() we will got NULL pointer dereference. e.g. #0 [ffffa25ec6978a38] machine_kexec at ffffffff8c669757 #1 [ffffa25ec6978a90] __crash_kexec at ffffffff8c7c0a4d #2 [ffffa25ec6978b58] crash_kexec at ffffffff8c7c1c48 #3 [ffffa25ec6978b60] oops_end at ffffffff8c627f2b #4 [ffffa25ec6978b80] page_fault_oops at ffffffff8c678fcb #5 [ffffa25ec6978bd8] exc_page_fault at ffffffff8d109542 #6 [ffffa25ec6978c00] asm_exc_page_fault at ffffffff8d200b62 [exception RIP: vxlan_ecn_decapsulate+0x3b] RIP: ffffffffc1014e7b RSP: ffffa25ec6978cb0 RFLAGS: 00010246 RAX: 0000000000000008 RBX: ffff8aa000888000 RCX: 0000000000000000 RDX: 000000000000000e RSI: ffff8a9fc7ab803e RDI: ffff8a9fd1168700 RBP: ffff8a9fc7ab803e R8: 0000000000700000 R9: 00000000000010ae R10: ffff8a9fcb748980 R11: 0000000000000000 R12: ffff8a9fd1168700 R13: ffff8aa000888000 R14: 00000000002a0000 R15: 00000000000010ae ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #7 [ffffa25ec6978ce8] vxlan_rcv at ffffffffc10189cd [vxlan] #8 [ffffa25ec6978d90] udp_queue_rcv_one_skb at ffffffff8cfb6507 #9 [ffffa25ec6978dc0] udp_unicast_rcv_skb at ffffffff8cfb6e45 #10 [ffffa25ec6978dc8] __udp4_lib_rcv at ffffffff8cfb8807 #11 [ffffa25ec6978e20] ip_protocol_deliver_rcu at ffffffff8cf76951 #12 [ffffa25ec6978e48] ip_local_deliver at ffffffff8cf76bde #13 [ffffa25ec6978ea0] __netif_receive_skb_one_core at ffffffff8cecde9b #14 [ffffa25ec6978ec8] process_backlog at ffffffff8cece139 #15 [ffffa25ec6978f00] __napi_poll at ffffffff8ceced1a #16 [ffffa25ec6978f28] net_rx_action at ffffffff8cecf1f3 #17 [ffffa25ec6978fa0] __softirqentry_text_start at ffffffff8d4000ca #18 [ffffa25ec6978ff0] do_softirq at ffffffff8c6fbdc3 Reproducer: https://github.com/Mellanox/ovs-tests/blob/master/test-ovs-vxlan-remove-tunnel-during-traffic.sh Fix this by waiting for all sk_user_data reader to finish before releasing the sock.	N/A	More Details
CVE-2022-50404	In the Linux kernel, the following vulnerability has been resolved: fbdev: fbcon: release buffer when fbcon_do_set_font() failed syzbot is reporting memory leak at fbcon_do_set_font() [1], for commit a5a923038d70 ("fbdev: fbcon: Properly revert changes when vc_resize() failed") missed that the buffer might be newly allocated by fbcon_set_font().	N/A	More Details
CVE-2023-53376	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Use number of bits to manage bitmap sizes To allocate bitmaps, the mpi3mr driver calculates sizes of bitmaps using byte as unit. However, bitmap helper functions assume that bitmaps are allocated using unsigned long as unit. This gap causes memory access beyond the bitmap sizes and results in "BUG: KASAN: slab-out-of-bounds". The BUG was observed at firmware download to eHBA-9600. Call trace indicated that the out-of-bounds access happened in find_first_zero_bit() called from mpi3mr_send_event_ack() for miroc->evtack_cmds_bitmap. To fix the BUG, do not use bytes to manage bitmap sizes. Instead, use number of bits, and call bitmap helper functions which take number of bits as arguments. For memory allocation, call bitmap_zalloc() instead of kzalloc() and krealloc(). For memory free, call bitmap_free() instead of kfree(). For zero clear, call bitmap_clear() instead of memset(). Remove three fields for bitmap byte sizes in struct scmd_priv which are no longer required. Replace the field dev_handle_bitmap_sz with dev_handle_bitmap_bits to keep number of bits of removepend_bitmap across resize.	N/A	More Details
CVE-2023-53394	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: xsk: Fix crash on regular rq reactivation When the regular rq is reactivated after the XSK socket is closed it could be reading stale cqes which eventually corrupts the rq. This leads to no more traffic being received on the regular rq and a crash on the next close or deactivation of the rq. Kal Cuttler Conely reported this issue as a crash on the release path when the xdpsock sample program is stopped (killed) and restarted in sequence while traffic is running. This patch flushes all cqes when during the rq flush. The cqe flushing is done in the reset state of the rq. mlx5e_rq_to_ready code is moved into the flush function to allow for this.	N/A	More Details
CVE-2025-57685	The LB-Link routers, including the BL-AC2100_AZ3 V1.0.4, BL-WR4000 v2.5.0, BL-WR9000_AE4 v2.4.9, BL-AC1900_AZ2 v1.0.2, BL-X26_AC8 v1.2.8, and BL-LTE300_DA4 V1.2.3 models, are vulnerable to unauthorized command injection. Attackers can exploit this vulnerability by accessing the /goform/set_serial_cfg interface to gain the highest level of device privileges without authorization, enabling them to remotely execute malicious commands.	N/A	More Details
CVE-2023-53396	In the Linux kernel, the following vulnerability has been resolved: ubifs: Fix memory leak in do_rename If renaming a file in an encrypted directory, function fscrypt_setup_filename allocates memory for a file name. This name is never used, and before returning to the caller the memory for it is not freed. When running kmemleak on it we see that it is registered as a leak. The report below is triggered by a simple program 'rename' that renames a file in an encrypted directory: unreferenced object 0xffff888101502840 (size 32): comm "rename", pid 9404, jiffies 4302582475 (age 435.735s) backtrace: __kmem_cache_alloc_node __kmalloc fscrypt_setup_filename do_rename ubifs_rename vfs_rename do_renameat2 To fix this we can remove the call to fscrypt_setup_filename as it's not needed.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: USB: sl811: fix memory leak with using		

2023-53417	debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53416	In the Linux kernel, the following vulnerability has been resolved: USB: isp1362: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53397	In the Linux kernel, the following vulnerability has been resolved: modpost: fix off by one in is_executable_section() The > comparison should be >= to prevent an out of bounds array access.	N/A	More Details
CVE-2023-53415	In the Linux kernel, the following vulnerability has been resolved: USB: dwc3: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once. Note, the root dentry for the debugfs directory for the device needs to be saved so we don't have to keep looking it up, which required a bit more refactoring to properly create and remove it when needed.	N/A	More Details
CVE-2023-53414	In the Linux kernel, the following vulnerability has been resolved: scsi: snic: Fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53398	In the Linux kernel, the following vulnerability has been resolved: mlx5: fix possible ptp queue fifo use-after-free Fifo indexes are not checked during pop operations and it leads to potential use-after-free when poping from empty queue. Such case was possible during re-sync action. WARN_ON_ONCE covers future cases. There were out-of-order cqe spotted which lead to drain of the queue and use-after-free because of lack of fifo pointers check. Special check and counter are added to avoid resync operation if SKB could not exist in the fifo because of OOO cqe (skb_id must be between consumer and producer index).	N/A	More Details
CVE-2023-53413	In the Linux kernel, the following vulnerability has been resolved: USB: isp116x: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53399	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix NULL pointer dereference in smb2_get_info_filesystem() If share is , share->path is NULL and it cause NULL pointer dereference issue.	N/A	More Details
CVE-2023-53412	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: bcm63xx_udc: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53411	In the Linux kernel, the following vulnerability has been resolved: PM: EM: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53400	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: Fix Oops by 9.1 surround channel names get_line_out_pfx() may trigger an Oops by overflowing the static array with more than 8 channels. This was reported for MacBookPro 12,1 with Cirrus codec. As a workaround, extend for the 9.1 channels and also fix the potential Oops by unifying the code paths accessing the same array with the proper size check.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: mm: kmem: fix a NULL pointer dereference in obj_stock_flush_required() KCSAN found an issue in obj_stock_flush_required(): stock->cached_objcg can be reset between the check and dereference: ========== BUG: KCSAN: data-race in drain_all_stock / drain_obj_stock write to 0xffff888237c2a2f8 of 8 bytes by task 19625 on cpu 0: drain_obj_stock+0x408/0x4e0 mm/memcontrol.c:3306 refill_obj_stock+0x9c/0x1e0 mm/memcontrol.c:3340 obj_cgroup_uncharge+0xe/0x10 mm/memcontrol.c:3408 memcg_slab_free_hook mm/slab.h:587 [inline] __cache_free mm/slab.c:3373 [inline] __do_kmem_cache_free mm/slab.c:3577 [inline] kmem_cache_free+0x105/0x280 mm/slab.c:3602 __d_free fs/dcache.c:298 [inline] dentry_free fs/dcache.c:375 [inline] __dentry_kill+0x422/0x4a0 fs/dcache.c:621 dentry_kill+0x8d/0x1e0 dput+0x118/0x1f0 fs/dcache.c:913 __fput+0x3bf/0x570 fs/file_table.c:329 ____fput+0x15/0x20 fs/file_table.c:349 task_work_run+0x123/0x160 kernel/task_work.c:179 resume_user_mode_work include/linux/resume_user_mode.h:49 [inline] exit_to_user_mode_loop+0xcf/0xe0 kernel/entry/common.c:171 exit_to_user_mode_prepare+0x6a/0xa0 kernel/entry/common.c:203 __syscall_exit_to_user_mode_work kernel/entry/common.c:285 [inline] syscall_exit_to_user_mode+0x26/0x140 kernel/entry/common.c:296		More

2023-53401	do_syscall_64+0x4d/0xc0 arch/x86/entry/common.c:86 entry_SYSCALL_64_after_hwframe+0x63/0xcd read to 0xffff888237c2a2f8 of 8 bytes by task 19632 on cpu 1: obj_stock_flush_required mm/memcontrol.c:3319 [inline] drain_all_stock+0x174/0x2a0 mm/memcontrol.c:2361 try_charge_memcg+0x6d0/0xd10 mm/memcontrol.c:2703 try_charge mm/memcontrol.c:2837 [inline] mem_cgroup_charge_skmem+0x51/0x140 mm/memcontrol.c:7290 sock_reserve_memory+0xb1/0x390 net/core/sock.c:1025 sk_setsockopt+0x800/0x1e70 net/core/sock.c:1525 udp_lib_setsockopt+0x99/0x6c0 net/ipv4/udp.c:2692 udp_setsockopt+0x73/0xa0 net/ipv4/udp.c:2817 sock_common_setsockopt+0x61/0x70 net/core/sock.c:3668 __sys_setsockopt+0x1c3/0x230 net/socket.c:2271 __do_sys_setsockopt net/socket.c:2282 [inline] __se_sys_setsockopt net/socket.c:2279 [inline] __x64_sys_setsockopt+0x66/0x80 net/socket.c:2279 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd value changed: 0xffff8881382d52c0 -> 0xffff888138893740 Reported by Kernel Concurrency Sanitizer on: CPU: 1 PID: 19632 Comm: syz-executor.0 Not tainted 6.3.0-rc2-syzkaller-00387-g534293368afa #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/02/2023 Fix it by using READ_ONCE()/WRITE_ONCE() for all accesses to stock->cached_objcg.	N/A	Details
CVE-2023-53410	In the Linux kernel, the following vulnerability has been resolved: USB: ULPI: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53409	In the Linux kernel, the following vulnerability has been resolved: drivers: base: component: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53408	In the Linux kernel, the following vulnerability has been resolved: trace/blktrace: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53407	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: pxa27x_udc: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53402	In the Linux kernel, the following vulnerability has been resolved: kernel/printk/index.c: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53403	In the Linux kernel, the following vulnerability has been resolved: time/debug: Fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53404	In the Linux kernel, the following vulnerability has been resolved: USB: fotg210: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53395	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Add AML_NO_OPERAND_RESOLVE flag to Timer ACPICA commit 90310989a0790032f5a0140741ff09b545af4bc5 According to the ACPI specification 19.6.134, no argument is required to be passed for ASL Timer instruction. For taking care of no argument, AML_NO_OPERAND_RESOLVE flag is added to ASL Timer instruction opcode. When ASL timer instruction interpreted by ACPI interpreter, getting error. After adding AML_NO_OPERAND_RESOLVE flag to ASL Timer instruction opcode, issue is not observed. == UBSAN: array-index-out-of-bounds in acpica/dswexec.c:401:12 index -1 is out of range for type 'union acpi_operand_object *[9]' CPU: 37 PID: 1678 Comm: cat Not tainted 6.0.0-dev-th500-6.0.y-1+bcf8c46459e407-generic-64k HW name: NVIDIA BIOS v1.1.1-d7acbfc-dirty 12/19/2022 Call trace: dump_backtrace+0xe0/0x130 show_stack+0x20/0x60 dump_stack_lvl+0x68/0x84 dump_stack+0x18/0x34 ubsan_epilogue+0x10/0x50 __ubsan_handle_out_of_bounds+0x80/0x90 acpi_ds_exec_end_op+0x1bc/0x6d8 acpi_ps_parse_loop+0x57c/0x618 acpi_ps_parse_aml+0x1e0/0x4b4 acpi_ps_execute_method+0x24c/0x2b8 acpi_ns_evaluate+0x3a8/0x4bc acpi_evaluate_object+0x15c/0x37c acpi_evaluate_integer+0x54/0x15c show_power+0x8c/0x12c [acpi_power_meter]	N/A	More Details
CVE-2025-55887	Cross-Site Scripting (XSS) vulnerability was discovered in the meal reservation service ARD. The vulnerability exists in the transactionID GET parameter on the transaction confirmation page. Due to improper input validation and output encoding, an attacker can inject malicious JavaScript code that is executed in the context of a user s browser. This can lead to session hijacking, theft of cookies, and other malicious actions	N/A	More Details

	performed on behalf of the victim.		
CVE-2023-53377	In the Linux kernel, the following vulnerability has been resolved: cifs: prevent use-after-free by freeing the cfile later In smb2_compound_op we have a possible use-after-free which can cause hard to debug problems later on. This was revealed during stress testing with KASAN enabled kernel. Fixing it by moving the cfile free call to a few lines below, after the usage.	N/A	More Details
CVE-2023-53418	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: lpc32xx_udc: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2023-53378	In the Linux kernel, the following vulnerability has been resolved: drm/i915/dpt: Treat the DPT BO as a framebuffer Currently i915_gem_object_is_framebuffer() doesn't treat the BO containing the framebuffer's DPT as a framebuffer itself. This means eg. that the shrinker can evict the DPT BO while leaving the actual FB BO bound, when the DPT is allocated from regular shmem. That causes an immediate oops during hibernate as we try to rewrite the PTEs inside the already evicted DPT obj. TODO: presumably this might also be the reason for the DPT related display faults under heavy memory pressure, but I'm still not sure how that would happen as the object should be pinned by intel_dpt_pin() while in active use by the display engine... (cherry picked from commit 779cb5ba64ec7df80675a956c9022929514f517a)	N/A	More Details
CVE-2023-53379	In the Linux kernel, the following vulnerability has been resolved: usb: phy: phy-tahvo: fix memory leak in tahvo_usb_probe() Smatch reports: drivers/usb/phy/phy-tahvo.c: tahvo_usb_probe() warn: missing unwind goto? After geting irq, if ret < 0, it will return without error handling to free memory. Just add error handling to fix this problem.	N/A	More Details
CVE-2023-53380	In the Linux kernel, the following vulnerability has been resolved: md/raid10: fix null-ptr-deref of mreplace in raid10_sync_request There are two check of 'mreplace' in raid10_sync_request(). In the first check, 'need_replace' will be set and 'mreplace' will be used later if no-Faulty 'mreplace' exists, In the second check, 'mreplace' will be set to NULL if it is Faulty, but 'need_replace' will not be changed accordingly. null-ptr-deref occurs if Faulty is set between two check. Fix it by merging two checks into one. And replace 'need_replace' with 'mreplace' because their values are always the same.	N/A	More Details
CVE-2023-53381	In the Linux kernel, the following vulnerability has been resolved: NFSD: fix leaked reference count of nfsd4_ssc_umount_item The reference count of nfsd4_ssc_umount_item is not decremented on error conditions. This prevents the laundromat from unmounting the vfsmount of the source file. This patch decrements the reference count of nfsd4_ssc_umount_item on error.	N/A	More Details
CVE-2023-53382	In the Linux kernel, the following vulnerability has been resolved: net/smc: Reset connection when trying to use SMCRv2 fails. We found a crash when using SMCRv2 with 2 Mellanox ConnectX-4. It can be reproduced by: - smc_run nginx - smc_run wrk -t 32 -c 500 -d 30 http://<ip>:<port> BUG: kernel NULL pointer dereference, address: 0000000000000014 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 8000000108713067 P4D 8000000108713067 PUD 151127067 PMD 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 4 PID: 2441 Comm: kworker/4:249 Kdump: loaded Tainted: G W E 6.4.0-rc1+ #42 Workqueue: smc_hs_wq smc_listen_work [smc] RIP: 0010:smc_clc_send_confirm_accept+0x284/0x580 [smc] RSP: 0018:ffffb8294b2d7c78 EFLAGS: 00010a06 RAX: ffff8f1873238880 RBX: ffffb8294b2d7dc8 RCX: 0000000000000000 RDX: 00000000000000b4 RSI: 0000000000000001 RDI: 0000000000b40c00 RBP: ffffb8294b2d7db8 R08: ffff8f1815c5860c R09: 0000000000000000 R10: 0000000000000400 R11: 0000000000000000 R12: ffff8f1846f56180 R13: ffff8f1815c5860c R14: 0000000000000001 R15: 0000000000000001 FS: 0000000000000000(0000) GS:ffff8f1aefd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000014 CR3: 00000001027a0001 CR4: 00000000003706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? mlx5_ib_map_mr_sg+0xa1/0xd0 [mlx5_ib] ? smcr_buf_map_link+0x24b/0x290 [smc] ? __smc_buf_create+0x4ee/0x9b0 [smc] smc_clc_send_accept+0x4c/0xb0 [smc] smc_listen_work+0x346/0x650 [smc] ? __schedule+0x279/0x820 process_one_work+0x1e5/0x3f0 worker_thread+0x4d/0x2f0 ? __pfx_worker_thread+0x10/0x10 kthread+0xe5/0x120 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2c/0x50 </TASK> During the CLC handshake, server sequentially tries available SMCRv2 and SMCRv1 devices in smc_listen_work(). If an SMCRv2 device is found. SMCv2 based link group and link will be assigned to the connection. Then assumed that some buffer assignment errors happen later in the CLC handshake, such as RMB registration failure, server will give up SMCRv2 and try SMCRv1 device instead. But the resources assigned to the connection won't be reset. When server tries SMCRv1 device, the connection creation process will be executed again. Since conn->lnk has been assigned when trying SMCRv2, it will not be set to the correct SMCRv1 link in smcr_lgr_conn_assign_link(). So in such situation, conn->lgr points to correct SMCRv1 link group but conn->lnk points to the SMCRv2 link mistakenly. Then in smc_clc_send_confirm_accept(), conn->rmb_desc->mr[link->link_idx] will be accessed. Since the link->link_idx is not correct, the related MR may not have been initialized, so crash happens. | Try SMCRv2 device first | |-> conn->lgr: assign existed SMCRv2 link group; | |-> conn->link: assign existed SMCRv2 link (link_idx may be 1 in SMC_LGR_SYMMETRIC); | |-> sndbuf & RMB creation fails, quit; | | Try SMCRv1 device then | |-> conn->lgr: create SMCRv1 link group and assign; | |-> conn->link: keep SMCRv2 link mistakenly; | |-> sndbuf & RMB creation succeed, only RMB->mr[link_idx =	N/A	More Details

	0] | initialized. | | Then smc_clc_send_confirm_accept() accesses | conn->rmb_desc->mr[conn->link->link_idx, which is 1], then crash. v This patch tries to fix this by cleaning conn->lnk before assigning link. In addition, it is better to reset the connection and clean the resources assigned if trying SMCRv2 failed in buffer creation or registration.		
CVE-2022-50403	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-50402	In the Linux kernel, the following vulnerability has been resolved: drivers/md/md-bitmap: check the return value of md_bitmap_get_counter() Check the return value of md_bitmap_get_counter() in case it returns NULL pointer, which will result in a null pointer dereference. v2: update the check to include other dereference	N/A	More Details
CVE-2023-53383	In the Linux kernel, the following vulnerability has been resolved: irqchip/gicv3: Workaround for NVIDIA erratum T241-FABRIC-4 The T241 platform suffers from the T241-FABRIC-4 erratum which causes unexpected behavior in the GIC when multiple transactions are received simultaneously from different sources. This hardware issue impacts NVIDIA server platforms that use more than two T241 chips interconnected. Each chip has support for 320 {E}SPIs. This issue occurs when multiple packets from different GICs are incorrectly interleaved at the target chip. The erratum text below specifies exactly what can cause multiple transfer packets susceptible to interleaving and GIC state corruption. GIC state corruption can lead to a range of problems, including kernel panics, and unexpected behavior. >From the erratum text: "In some cases, inter-socket AXI4 Stream packets with multiple transfers, may be interleaved by the fabric when presented to ARM Generic Interrupt Controller. GIC expects all transfers of a packet to be delivered without any interleaving. The following GICv3 commands may result in multiple transfer packets over inter-socket AXI4 Stream interface: - Register reads from GICD_I* and GICD_N* - Register writes to 64-bit GICD registers other than GICD_IROUTERn* - ITS command MOVALL Multiple commands in GICv4+ utilize multiple transfer packets, including VMOVP, VMOVI, VMAPP, and 64-bit register accesses." This issue impacts system configurations with more than 2 sockets, that require multi-transfer packets to be sent over inter-socket AXI4 Stream interface between GIC instances on different sockets. GICv4 cannot be supported. GICv3 SW model can only be supported with the workaround. Single and Dual socket configurations are not impacted by this issue and support GICv3 and GICv4." Writing to the chip alias region of the GICD_In{E} registers except GICD_ICENABLERn has an equivalent effect as writing to the global distributor. The SPI interrupt deactivate path is not impacted by the erratum. To fix this problem, implement a workaround that ensures read accesses to the GICD_In{E} registers are directed to the chip that owns the SPI, and disable GICv4.x features. To simplify code changes, the gic_configure_irq() function uses the same alias region for both read and write operations to GICD_ICFGR.	N/A	More Details
CVE-2022-50401	In the Linux kernel, the following vulnerability has been resolved: nfsd: under NFSv4.1, fix double svc_xprt_put on rpc_create failure On error situation `clp->cl_cb_conn.cb_xprt` should not be given a reference to the xprt otherwise both client cleanup and the error handling path of the caller call to put it. Better to delay handing over the reference to a later branch. [72.530665] refcount_t: underflow; use-after-free. [72.531933] WARNING: CPU: 0 PID: 173 at lib/refcount.c:28 refcount_warn_saturate+0xcf/0x120 [72.533075] Modules linked in: nfsd(OE) nfsv4(OE) nfsv3(OE) nfs(OE) lockd(OE) compat_nfs_ssc(OE) nfs_acl(OE) rpcsec_gss_krb5(OE) auth_rpcgss(OE) rpcrdma(OE) dns_resolver fscache netfs grace rdma_cm iw_cm ib_cm sunrpc(OE) mlx5_ib mlx5_core mlxfw pci_hyperv_intf ib_uverbs ib_core xt_MASQUERADE nf_conntrack_netlink nft_counter xt_addrtype nft_compat br_netfilter bridge stp llc nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set overlay nf_tables nfnetlink crct10dif_pclmul crc32_pclmul ghash_clmulni_intel xfs serio_raw virtio_net virtio_blk net_failover failover fuse [last unloaded: sunrpc] [72.540389] CPU: 0 PID: 173 Comm: kworker/u16:5 Tainted: G OE 5.15.82-dan #1 [72.541511] Hardware name: Red Hat KVM/RHEL-AV, BIOS 1.16.0-3.module+el8.7.0+1084+97b81f61 04/01/2014 [72.542717] Workqueue: nfsd4_callbacks nfsd4_run_cb_work [nfsd] [72.543575] RIP: 0010:refcount_warn_saturate+0xcf/0x120 [72.544299] Code: 55 00 0f 0b 5d e9 01 50 98 00 80 3d 75 9e 39 08 00 0f 85 74 ff ff ff 48 c7 c7 e8 d1 60 8e c6 05 61 9e 39 08 01 e8 f6 51 55 00 <0f> 0b 5d e9 d9 4f 98 00 80 3d 4b 9e 39 08 00 0f 85 4c ff ff ff 48 [72.546666] RSP: 0018:ffffb3f841157cf0 EFLAGS: 00010286 [72.547393] RAX: 0000000000000026 RBX: ffff89ac6231d478 RCX: 0000000000000000 [72.548324] RDX: ffff89adb7c2c2c0 RSI: ffff89adb7c205c0 RDI: ffff89adb7c205c0 [72.549271] RBP: ffffb3f841157cf0 R08: 0000000000000000 R09: c0000000ffefffff [72.550209] R10: 0000000000000001 R11: ffffb3f841157ad0 R12: ffff89ac6231d180 [72.551142] R13: ffff89ac6231d478 R14: ffff89ac40c06180 R15: ffff89ac6231d4b0 [72.552089] FS: 0000000000000000(0000) GS:ffff89adb7c00000(0000) knlGS:0000000000000000 [72.553175] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [72.553934] CR2: 0000563a310506a8 CR3: 0000000109a66000 CR4: 0000000000350ef0 [72.554874] Call Trace: [72.555278] <TASK> [72.555614] svc_xprt_put+0xaf/0xe0 [sunrpc] [72.556276] nfsd4_process_cb_update.isra.11+0xb7/0x410 [nfsd] [72.557087] ? update_load_avg+0x82/0x610 [72.557652] ? cpuacct_charge+0x60/0x70 [72.558212] ? dequeue_entity+0xdb/0x3e0 [72.558765] ? queued_spin_unlock+0x9/0x20 [72.559358] nfsd4_run_cb_work+0xfc/0x270 [nfsd] [72.560031] process_one_work+0x1df/0x390 [72.560600] worker_thread+0x37/0x3b0 [72.561644] ? process_one_work+0x390/0x390 [72.562247] kthread+0x12f/0x150 [72.562710] ? set_kthread_struct+0x50/0x50 [72.563309] ret_from_fork+0x22/0x30 [72.563818] </TASK> [72.564189] ---[end trace 031117b1c72ec616]--- [72.566019] list_add corruption. next->prev should be prev (ffff89ac4977e538), but was ffff89ac4763e018. (next=ffff89ac4763e018). [72.567647] ------------[cut here]------------	N/A	More Details

CVE-2025-59421	Press, a Frappe custom app that runs Frappe Cloud, manages infrastructure, subscription, marketplace, and software-as-a-service (SaaS). A bad actor can flood the inbox of a user by repeatedly sending invites (duplicate). The issue is fixed in commit 83c3fc7676c5dbbe1fd5092d21d95a10c7b48615.	N/A	More Details
CVE-2023-53384	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: avoid possible NULL skb pointer dereference In 'mwifiex_handle_uap_rx_forward()', always check the value returned by 'skb_copy()' to avoid potential NULL pointer dereference in 'mwifiex_uap_queue_bridged_pkt()', and drop original skb in case of copying failure. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2023-53385	In the Linux kernel, the following vulnerability has been resolved: media: mdp3: Fix resource leaks in of_find_device_by_node Use put_device to release the object get through of_find_device_by_node, avoiding resource leaks.	N/A	More Details
CVE-2023-53386	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix potential use-after-free when clear keys Similar to commit c5d2b6fa26b5 ("Bluetooth: Fix use-after-free in hci_remove_ltk/hci_remove_irk"). We can not access k after kfree_rcu() call.	N/A	More Details
CVE-2023-53387	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix device management cmd timeout flow In the UFS error handling flow, the host will send a device management cmd (NOP OUT) to the device for link recovery. If this cmd times out and clearing the doorbell fails, ufshcd_wait_for_dev_cmd() will do nothing and return. hba->dev_cmd.complete struct is not set to NULL. When this happens, if cmd has been completed by device, then we will call complete() in __ufshcd_transfer_req_compl(). Because the complete struct is allocated on the stack, the following crash will occur: ipanic_die+0x24/0x38 [mrdump] die+0x344/0x748 arm64_notify_die+0x44/0x104 do_debug_exception+0x104/0x1e0 el1_dbg+0x38/0x54 el1_sync_handler+0x40/0x88 el1_sync+0x8c/0x140 queued_spin_lock_slowpath+0x2e4/0x3c0 __ufshcd_transfer_req_compl+0x3b0/0x1164 ufshcd_trc_handler+0x15c/0x308 ufshcd_host_reset_and_restore+0x54/0x260 ufshcd_reset_and_restore+0x28c/0x57c ufshcd_err_handler+0xeb8/0x1b6c process_one_work+0x288/0x964 worker_thread+0x4bc/0xc7c kthread+0x15c/0x264 ret_from_fork+0x10/0x30	N/A	More Details
CVE-2023-53388	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Clean dangling pointer on bind error path mtk_drm_bind() can fail, in which case drm_dev_put() is called, destroying the drm_device object. However a pointer to it was still being held in the private object, and that pointer would be passed along to DRM in mtk_drm_sys_prepare() if a suspend were triggered at that point, resulting in a panic. Clean the pointer when destroying the object in the error path to prevent this from happening.	N/A	More Details
CVE-2023-53389	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: dp: Only trigger DRM HPD events if bridge is attached The MediaTek DisplayPort interface bridge driver starts its interrupts as soon as its probed. However when the interrupts trigger the bridge might not have been attached to a DRM device. As drm_helper_hpd_irq_event() does not check whether the passed in drm_device is valid or not, a NULL pointer passed in results in a kernel NULL pointer dereference in it. Check whether the bridge is attached and only trigger an HPD event if it is.	N/A	More Details
CVE-2023-53390	In the Linux kernel, the following vulnerability has been resolved: drivers: base: dd: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2025-59417	Lobe Chat is an open-source artificial intelligence chat framework. Prior to version 1.129.4, there is a a cross-site scripting (XSS) vulnerability when handling chat message in lobe-chat that can be escalated to remote code execution on the user's machine. In lobe-chat, when the response from the server is like <lobeArtifact identifier="ai-new-interpretation" ...> , it will be rendered with the lobeArtifact node, instead of the plain text. However, when the type of the lobeArtifact is image/svg+xml , it will be rendered as the SVGRender component, which internally uses dangerouslySetInnerHTML to set the content of the svg, resulting in XSS attack. Any party capable of injecting content into chat messages, such as hosting a malicious page for prompt injection, operating a compromised MCP server, or leveraging tool integrations, can exploit this vulnerability. This vulnerability is fixed in 1.129.4.	N/A	More Details
CVE-2023-53391	In the Linux kernel, the following vulnerability has been resolved: shmem: use ramfs_kill_sb() for kill_sb method of ramfs-based tmpfs As the ramfs-based tmpfs uses ramfs_init_fs_context() for the init_fs_context method, which allocates fc->s_fs_info, use ramfs_kill_sb() to free it and avoid a memory leak.	N/A	More Details
CVE-2023-53392	In the Linux kernel, the following vulnerability has been resolved: HID: intel-ish-hid: Fix kernel panic during warm reset During warm reset device->fw_client is set to NULL. If a bus driver is registered after this NULL setting and before new firmware clients are enumerated by ISHTP, kernel panic will result in the function ishtp_cl_bus_match(). This is because of reference to device->fw_client->props.protocol_name. ISH firmware after getting successfully loaded, sends a warm reset notification to remove all clients from the bus and sets device->fw_client to NULL. Until kernel v5.15, all enabled ISHTP kernel module drivers were loaded right after any of the first ISHTP device was registered, regardless of whether it was a matched or an unmatched device. This resulted in all drivers getting registered much before the warm reset notification from ISH. Starting kernel v5.16, this issue got exposed after the change was introduced to load only bus drivers for the	N/A	More Details

	respective matching devices. In this scenario, cros_ec_ishtp device and cros_ec_ishtp driver are registered after the warm reset device fw_client NULL setting. cros_ec_ishtp driver_register() triggers the callback to ishtp_cl_bus_match() to match ISHTP driver to the device and causes kernel panic in guid_equal() when dereferencing fw_client NULL pointer to get protocol_name.		
CVE-2023-53393	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix mlx5_ib_get_hw_stats when used for device Currently, when mlx5_ib_get_hw_stats() is used for device (port_num = 0), there is a special handling in order to use the correct counters, but, port_num is being passed down the stack without any change. Also, some functions assume that port_num >=1. As a result, the following oops can occur. BUG: unable to handle page fault for address: ffff89510294f1a8 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] SMP CPU: 8 PID: 1382 Comm: devlink Tainted: G W 6.1.0-rc4_for_upstream_base_2022_11_10_16_12 #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 RIP: 0010:_raw_spin_lock+0xc/0x20 Call Trace: <TASK> mlx5_ib_get_native_port_mdev+0x73/0xe0 [mlx5_ib] do_get_hw_stats.constprop.0+0x109/0x160 [mlx5_ib] mlx5_ib_get_hw_stats+0xad/0x180 [mlx5_ib] ib_setup_device_attrs+0xf0/0x290 [ib_core] ib_register_device+0x3bb/0x510 [ib_core] ? atomic_notifier_chain_register+0x67/0x80 __mlx5_ib_add+0x2b/0x80 [mlx5_ib] mlx5r_probe+0xb8/0x150 [mlx5_ib] ? auxiliary_match_id+0x6a/0x90 auxiliary_bus_probe+0x3c/0x70 ? driver_sysfs_add+0x6b/0x90 really_probe+0xcd/0x380 __driver_probe_device+0x80/0x170 driver_probe_device+0x1e/0x90 __device_attach_driver+0x7d/0x100 ? driver_allows_async_probing+0x60/0x60 ? driver_allows_async_probing+0x60/0x60 bus_for_each_drv+0x7b/0xc0 __device_attach+0xbc/0x200 bus_probe_device+0x87/0xa0 device_add+0x404/0x940 ? dev_set_name+0x53/0x70 __auxiliary_device_add+0x43/0x60 add_adev+0x99/0xe0 [mlx5_core] mlx5_attach_device+0xc8/0x120 [mlx5_core] mlx5_load_one_devl_locked+0xb2/0xe0 [mlx5_core] devlink_reload+0x133/0x250 devlink_nl_cmd_reload+0x480/0x570 ? devlink_nl_pre_doit+0x44/0x2b0 genl_family_rcv_msg_doit.isra.0+0xc2/0x110 genl_rcv_msg+0x180/0x2b0 ? devlink_nl_cmd_region_read_dumpit+0x540/0x540 ? devlink_reload+0x250/0x250 ? devlink_put+0x50/0x50 ? genl_family_rcv_msg_doit.isra.0+0x110/0x110 netlink_rcv_skb+0x54/0x100 genl_rcv+0x24/0x40 netlink_unicast+0x1f6/0x2c0 netlink_sendmsg+0x237/0x490 sock_sendmsg+0x33/0x40 __sys_sendto+0x103/0x160 ? handle_mm_fault+0x10e/0x290 ? do_user_addr_fault+0x1c0/0x5f0 __x64_sys_sendto+0x25/0x30 do_syscall_64+0x3d/0x90 entry_SYSCALL_64_after_hwframe+0x46/0xb0 Fix it by setting port_num to 1 in order to get device status and remove unused variable.	N/A	More Details
CVE-2022-50387	In the Linux kernel, the following vulnerability has been resolved: net: hinic: fix the issue of CMDQ memory leaks When hinic_set_cmdq_depth() fails in hinic_init_cmdqs(), the cmdq memory is not released correctly. Fix it.	N/A	More Details
CVE-2022-50385	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix an Oops in nfs_d_automount() When mounting from a NFSv4 referral, path->dentry can end up being a negative dentry, so derive the struct nfs_server from the dentry itself instead.	N/A	More Details
CVE-2025-39839	In the Linux kernel, the following vulnerability has been resolved: batman-adv: fix OOB read/write in network-coding decode batadv_nc_skb_decode_packet() trusts coded_len and checks only against skb->len. XOR starts at sizeof(struct batadv_unicast_packet), reducing payload headroom, and the source skb length is not verified, allowing an out-of-bounds read and a small out-of-bounds write. Validate that coded_len fits within the payload area of both destination and source sk_buffs before XORing.	N/A	More Details
CVE-2025-7979	Ashlar-Vellum Graphite VC6 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25463.	N/A	More Details
CVE-2025-59672	Rejected reason: Not used	N/A	More Details
CVE-2025-59671	Rejected reason: Not used	N/A	More Details
CVE-2025-59670	Rejected reason: Not used	N/A	More Details
CVE-2025-10643	Wondershare Repairit Incorrect Permission Assignment Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of Wondershare Repairit. Authentication is not required to exploit this vulnerability. The specific flaw exists within the permissions granted to a storage account token. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-26902.	N/A	More Details

CVE-2025-10644	Wondershare Repairit SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on Wondershare Repairit. Authentication is not required to exploit this vulnerability. The specific flaw exists within the permissions granted to an SAS token. An attacker can leverage this vulnerability to launch a supply-chain attack and execute arbitrary code on customers' endpoints. Was ZDI-CAN-26892.	N/A	More Details
CVE-2025-47698	An adjacent attacker without authentication can exploit this vulnerability to retrieve a set of user-privileged credentials. These credentials are present during the firmware upgrade procedure.	N/A	More Details
CVE-2025-7977	Ashlar-Vellum Cobalt LI File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of LI files. The issue results from the lack of proper validation of user-supplied data, which can result in a read before the start of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25354.	N/A	More Details
CVE-2025-10650	SoftIron HyperCloud 2.5.0 through 2.6.3 may incorrectly add user SSH keys to the administrator-level authorized keys under certain conditions, allowing unauthorized privilege escalation to admin via SSH.	N/A	More Details
CVE-2023-53447	In the Linux kernel, the following vulnerability has been resolved: f2fs: don't reset unchangable mount option in f2fs_remount() syzbot reports a bug as below: general protection fault, probably for non-canonical address 0xdfffffc0000000009: 0000 [#1] PREEMPT SMP KASAN RIP: 0010:__lock_acquire+0x69/0x2000 kernel/locking/lockdep.c:4942 Call Trace: lock_acquire+0x1e3/0x520 kernel/locking/lockdep.c:5691 __raw_write_lock include/linux/rwlock_api_smp.h:209 [inline] _raw_write_lock+0x2e/0x40 kernel/locking/spinlock.c:300 __drop_extent_tree+0x3ac/0x660 fs/f2fs/extent_cache.c:1100 f2fs_drop_extent_tree+0x17/0x30 fs/f2fs/extent_cache.c:1116 f2fs_insert_range+0x2d5/0x3c0 fs/f2fs/file.c:1664 f2fs_fallocate+0x4e4/0x6d0 fs/f2fs/file.c:1838 vfs_fallocate+0x54b/0x6b0 fs/open.c:324 ksys_fallocate fs/open.c:347 [inline] __do_sys_fallocate fs/open.c:355 [inline] __se_sys_fallocate fs/open.c:353 [inline] __x64_sys_fallocate+0xbd/0x100 fs/open.c:353 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd The root cause is race condition as below: - since it tries to remount rw filesystem, so that do_remount won't call sb_prepare_remount_readonly to block fallocate, there may be race condition in between remount and fallocate. - in f2fs_remount(), default_options() will reset mount option to default one, and then update it based on result of parse_options(), so there is a hole which race condition can happen. Thread A Thread B - f2fs_fill_super - parse_options - clear_opt(READ_EXTENT_CACHE) - f2fs_remount - default_options - set_opt(READ_EXTENT_CACHE) - f2fs_fallocate - f2fs_insert_range - f2fs_drop_extent_tree - __drop_extent_tree - __may_extent_tree - test_opt(READ_EXTENT_CACHE) return true - write_lock(&et->lock) access NULL pointer - parse_options - clear_opt(READ_EXTENT_CACHE)	N/A	More Details
CVE-2025-7978	Ashlar-Vellum Graphite VC6 File Parsing Uninitialized Variable Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25459.	N/A	More Details
CVE-2025-7980	Ashlar-Vellum Graphite VC6 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25465.	N/A	More Details
CVE-2022-50384	In the Linux kernel, the following vulnerability has been resolved: staging: vme_user: Fix possible UAF in tsi148_dma_list_add Smatch report warning as follows: drivers/staging/vme_user/vme_tsi148.c:1757 tsi148_dma_list_add() warn: '&entry->list' not removed from list In tsi148_dma_list_add(), the error path "goto err_dma" will not remove entry->list from list->entries, but entry will be freed, then list traversal may cause UAF. Fix by removeing it from list->entries before free().	N/A	More Details
CVE-2025-7981	Ashlar-Vellum Graphite VC6 File Parsing Uninitialized Variable Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25475.	N/A	More Details
	Ashlar-Vellum Cobalt LI File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User		

CVE-2025-7982	interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of LI files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25476.	N/A	More Details
CVE-2025-7983	Ashlar-Vellum Graphite VC6 File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25477.	N/A	More Details
CVE-2025-10009	Incorrect handling of uploaded files in the admin "Restore" function in Invoice Ninja <= 5.11.72 allows attackers with admin credentials to execute arbitrary code on the server via uploaded .php files.	N/A	More Details
CVE-2025-7984	Ashlar-Vellum Cobalt AR File Parsing Uninitialized Variable Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25700.	N/A	More Details
CVE-2025-7985	Ashlar-Vellum Cobalt VC6 File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25704.	N/A	More Details
CVE-2025-7986	Ashlar-Vellum Graphite VC6 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25755.	N/A	More Details
CVE-2025-7987	Ashlar-Vellum Graphite VC6 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25756.	N/A	More Details
CVE-2025-7988	Ashlar-Vellum Graphite VC6 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Graphite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25862.	N/A	More Details
CVE-2025-7989	Ashlar-Vellum Cobalt AR File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25943.	N/A	More Details
CVE-2025-59673	Rejected reason: Not used	N/A	More Details
CVE-2025-59674	Rejected reason: Not used	N/A	More Details

CVE-2025-59675	Rejected reason: Not used	N/A	More Details
CVE-2025-59676	Rejected reason: Not used	N/A	More Details
CVE-2025-39838	In the Linux kernel, the following vulnerability has been resolved: cifs: prevent NULL pointer dereference in UTF16 conversion There can be a NULL pointer dereference bug here. NULL is passed to __cifs_sfu_make_node without checks, which passes it unchecked to cifs_strndup_to_utf16, which in turn passes it to cifs_local_to_utf16_bytes where '*from' is dereferenced, causing a crash. This patch adds a check for NULL 'src' in cifs_strndup_to_utf16 and returns NULL early to prevent dereferencing NULL pointer. Found by Linux Verification Center (linuxtesting.org) with SVACE	N/A	More Details
CVE-2025-59431	MapServer is a system for developing web-based GIS applications. Prior to 8.4.1, the XML Filter Query directive PropertyName is vulnerably to Boolean-based SQL injection. It seems like expression checking is bypassed by introducing double quote characters in the PropertyName. Allowing to manipulate backend database queries. This vulnerability is fixed in 8.4.1.	N/A	More Details
CVE-2025-39837	In the Linux kernel, the following vulnerability has been resolved: platform/x86: asus-wmi: Fix racy registrations asus_wmi_register_driver() may be called from multiple drivers concurrently, which can lead to the racy list operations, eventually corrupting the memory and hitting Oops on some ASUS machines. Also, the error handling is missing, and it forgot to unregister ACPI lps0 dev ops in the error case. This patch covers those issues by introducing a simple mutex at acpi_wmi_register_driver() & *_unregister_driver, and adding the proper call of asus_s2idle_check_unregister() in the error path.	N/A	More Details
CVE-2023-53406	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: pxa25x_udc: fix memory leak with using debugfs_lookup() When calling debugfs_lookup() the result must have dput() called on it, otherwise the memory will leak over time. To make things simpler, just call debugfs_lookup_and_remove() instead which handles all of the logic at once.	N/A	More Details
CVE-2025-43808	The Commerce component in Liferay Portal 7.3.0 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and 7.3 service pack 3 through update 35 saves virtual products uploaded to Documents and Media with guest view permission, which allows remote attackers to access and download virtual products for free via a crafted URL.	N/A	More Details
CVE-2025-59720	Rejected reason: Not used	N/A	More Details
CVE-2025-59721	Rejected reason: Not used	N/A	More Details
CVE-2025-59722	Rejected reason: Not used	N/A	More Details
CVE-2025-59723	Rejected reason: Not used	N/A	More Details
CVE-2025-59724	Rejected reason: Not used	N/A	More Details
CVE-2025-59725	Rejected reason: Not used	N/A	More Details
CVE-2025-59726	Rejected reason: Not used	N/A	More Details
CVE-2025-59341	esm.sh is a nobuild content delivery network(CDN) for modern web development. In 136 and earlier, a Local File Inclusion (LFI) issue was identified in the esm.sh service URL handling. An attacker could craft a request that causes the server to read and return files from the host filesystem (or other unintended file sources).	N/A	More Details
CVE-2025-59342	esm.sh is a nobuild content delivery network(CDN) for modern web development. In 136 and earlier, a path-traversal flaw in the handling of the X-Zone-Id HTTP header allows an attacker to cause the application to write files outside the intended storage location. The header value is used to build a filesystem path but is not properly canonicalized or restricted to the application’s storage base directory. As a result, supplying ../	N/A	More Details

	sequences in X-Zone-Id causes files to be written to arbitrary directories.		
CVE-2025-59345	Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, The /api/v1/jobs and /preheats endpoints in Manager web UI are accessible without authentication. Any user with network access to the Manager can create, delete, and modify jobs, and create preheat jobs. An unauthenticated adversary with network access to a Manager web UI uses /api/v1/jobs endpoint to create hundreds of useless jobs. The Manager is in a denial-of-service state, and stops accepting requests from valid administrators. This vulnerability is fixed in 2.1.0.	N/A	More Details
CVE-2025-59727	Rejected reason: Not used	N/A	More Details
CVE-2024-10246	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-59416	The Scratch Channel is a news website. If the user makes a fork, they can change the admins and make an article. Since the API uses a POST request, it will make an article. This issue is fixed in v1.2.	N/A	More Details
CVE-2025-6544	A deserialization vulnerability exists in h2oai/h2o-3 versions <= 3.46.0.8, allowing attackers to read arbitrary system files and execute arbitrary code. The vulnerability arises from improper handling of JDBC connection parameters, which can be exploited by bypassing regular expression checks and using double URL encoding. This issue impacts all users of the affected versions.	N/A	More Details
CVE-2025-59678	Rejected reason: Not used	N/A	More Details
CVE-2025-59677	Rejected reason: Not used	N/A	More Details
CVE-2025-7990	Ashlar-Vellum Cobalt VC6 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25944.	N/A	More Details
CVE-2025-7991	Ashlar-Vellum Cobalt VC6 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VC6 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25945.	N/A	More Details
CVE-2025-7992	Ashlar-Vellum Cobalt AR File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25972.	N/A	More Details
CVE-2023-53438	In the Linux kernel, the following vulnerability has been resolved: x86/MCE: Always save CS register on AMD Zen IF Poison errors The Instruction Fetch (IF) units on current AMD Zen-based systems do not guarantee a synchronous #MC is delivered for poison consumption errors. Therefore, MCG_STATUS[EIPV|RIPV] will not be set. However, the microarchitecture does guarantee that the exception is delivered within the same context. In other words, the exact rIP is not known, but the context is known to not have changed. There is no architecturally-defined method to determine this behavior. The Code Segment (CS) register is always valid on such IF unit poison errors regardless of the value of MCG_STATUS[EIPV|RIPV]. Add a quirk to save the CS register for poison consumption from the IF unit banks. This is needed to properly determine the context of the error. Otherwise, the severity grading function will assume the context is IN_KERNEL due to the m->cs value being 0 (the initialized value). This leads to unnecessary kernel panics on data poison errors due to the kernel believing the poison consumption occurred in kernel context.	N/A	More Details
CVE-2023-	In the Linux kernel, the following vulnerability has been resolved: scsi: snic: Fix possible memory leak if device_add() fails If device_add() returns error, the name allocated by dev_set_name() needs be freed. As the	N/A	More

53436	comment of device_add() says, put_device() should be used to give up the reference in the error path. So fix this by calling put_device(), then the name can be freed in kobject_cleanp().		Details
CVE-2023-53435	In the Linux kernel, the following vulnerability has been resolved: cassini: Fix a memory leak in the error handling path of cas_init_one() cas_saturn_firmware_init() allocates some memory using vmalloc(). This memory is freed in the .remove() function but not it the error handling path of the probe. Add the missing vfree() to avoid a memory leak, should an error occur.	N/A	More Details
CVE-2023-53434	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_dsp_rproc: Add custom memory copy implementation for i.MX DSP Cores The IRAM is part of the HiFi DSP. According to hardware specification only 32-bits write are allowed otherwise we get a Kernel panic. Therefore add a custom memory copy and memset functions to deal with the above restriction.	N/A	More Details
CVE-2025-40677	SQL injection vulnerability in Summar Software´s Portal del Empleado. This vulnerability allows an attacker to retrieve, create, update, and delete the database by sending a POST request using the parameter “ctl00$ContentPlaceHolder1$filtroNombre” in “/MemberPages/quienesquien.aspx”.	N/A	More Details
CVE-2025-9038	Improper Privilege Management vulnerability in GE Vernova S1 Agile Configuration Software on Windows allows Privilege Escalation.This issue affects S1 Agile Configuration Software: 3.1 and previous version.	N/A	More Details
CVE-2023-53433	In the Linux kernel, the following vulnerability has been resolved: net: add vlan_get_protocol_and_depth() helper Before blamed commit, pskb_may_pull() was used instead of skb_header_pointer() in __vlan_get_protocol() and friends. Few callers depended on skb->head being populated with MAC header, syzbot caught one of them (skb_mac_gso_segment()) Add vlan_get_protocol_and_depth() to make the intent clearer and use it where sensible. This is a more generic fix than commit e9d3f80935b6 ("net/af_packet: make sure to pull mac header") which was dealing with a similar issue. kernel BUG at include/linux/skbuff.h:2655 ! invalid opcode: 0000 [#1] SMP KASAN CPU: 0 PID: 1441 Comm: syz-executor199 Not tainted 6.1.24-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/14/2023 RIP: 0010:__skb_pull include/linux/skbuff.h:2655 [inline] RIP: 0010:skb_mac_gso_segment+0x68f/0x6a0 net/core/gro.c:136 Code: fd 48 8b 5c 24 10 44 89 6b 70 48 c7 c7 c0 ae 0d 86 44 89 e6 e8 a1 91 d0 00 48 c7 c7 00 af 0d 86 48 89 de 31 d2 e8 d1 4a e9 ff <0f> 0b 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 55 48 89 e5 41 RSP: 0018:ffffc90001bd7520 EFLAGS: 00010286 RAX: ffffffff8469736a RBX: ffff88810f31dac0 RCX: ffff888115a18b00 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc90001bd75e8 R08: ffffffff84697183 R09: fffff5200037adf9 R10: 0000000000000000 R11: dfffffc0000000001 R12: 0000000000000012 R13: 000000000000fee5 R14: 0000000000005865 R15: 000000000000fed7 FS: 000055555633f300(0000) GS:ffff8881f6a00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000000 CR3: 0000000116fea000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> [<ffffffff847018dd>] __skb_gso_segment+0x32d/0x4c0 net/core/dev.c:3419 [<ffffffff8470398a>] skb_gso_segment include/linux/netdevice.h:4819 [inline] [<ffffffff8470398a>] validate_xmit_skb+0x3aa/0xee0 net/core/dev.c:3725 [<ffffffff84707042>] __dev_queue_xmit+0x1332/0x3300 net/core/dev.c:4313 [<ffffffff851a9ec7>] dev_queue_xmit+0x17/0x20 include/linux/netdevice.h:3029 [<ffffffff851b4a82>] packet_snd net/packet/af_packet.c:3111 [inline] [<ffffffff851b4a82>] packet_sendmsg+0x49d2/0x6470 net/packet/af_packet.c:3142 [<ffffffff84669a12>] sock_sendmsg_nosec net/socket.c:716 [inline] [<ffffffff84669a12>] sock_sendmsg net/socket.c:736 [inline] [<ffffffff84669a12>] __sys_sendto+0x472/0x5f0 net/socket.c:2139 [<ffffffff84669c75>] __do_sys_sendto net/socket.c:2151 [inline] [<ffffffff84669c75>] __se_sys_sendto net/socket.c:2147 [inline] [<ffffffff84669c75>] __x64_sys_sendto+0xe5/0x100 net/socket.c:2147 [<ffffffff8551d40f>] do_syscall_x64 arch/x86/entry/common.c:50 [inline] [<ffffffff8551d40f>] do_syscall_64+0x2f/0x50 arch/x86/entry/common.c:80 [<ffffffff85600087>] entry_SYSCALL_64_after_hwframe+0x63/0xcd	N/A	More Details
CVE-2025-40678	Unrestricted upload vulnerability for dangerous file types on Summar Software´s Portal del Empleado. This vulnerability allows an attacker to upload a dangerous file type by sending a POST request using the parameter “cctl00$ContentPlaceHolder1$fuAdjunto” in “/MemberPages/ntf_absentismo.aspx”.	N/A	More Details
CVE-2023-53432	In the Linux kernel, the following vulnerability has been resolved: firewire: net: fix use after free in fwnet_finish_incoming_packet() The netif_rx() function frees the skb so we can't dereference it to save the skb->len.	N/A	More Details
CVE-2023-53431	In the Linux kernel, the following vulnerability has been resolved: scsi: ses: Don't attach if enclosure has no components An enclosure with no components can't usefully be operated by the driver (since effectively it has nothing to manage), so report the problem and don't attach. Not attaching also fixes an oops which could occur if the driver tries to manage a zero component enclosure. [mkp: Switched to KERN_WARNING since this scenario is common]	N/A	More Details
CVE-2023-53430	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: dma: fix memory leak running mt76_dma_tx_cleanup Fix device unregister memory leak and alway cleanup all configured rx queues in mt76_dma_tx_cleanup routine.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: tty: serial: fsl_lpuart: disable dma rx/tx use		

CVE-2022-50375	flags in lpuart_dma_shutdown lpuart_dma_shutdown tears down lpuart dma, but lpuart_flush_buffer can still occur which in turn tries to access dma apis if lpuart_dma_tx_use flag is true. At this point since dma is torn down, these dma apis can abort. Set lpuart_dma_tx_use and the corresponding rx flag lpuart_dma_rx_use to false in lpuart_dma_shutdown so that dmas are not accessed after they are relinquished. Otherwise, when try to kill btattach, kernel may panic. This patch may fix this issue. root@imx8ulpevk:~# btattach -B /dev/ttyLP2 -S 115200 ^C[90.182296] Internal error: synchronous external abort: 96000210 [#1] PREEMPT SMP [90.189806] Modules linked in: moal(O) mlan(O) [90.194258] CPU: 0 PID: 503 Comm: btattach Tainted: G O 5.15.32-06136-g34eecdf2f9e4 #37 [90.203554] Hardware name: NXP i.MX8ULP 9X9 EVK (DT) [90.208513] pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [90.215470] pc : fsl_edma3_disable_request+0x8/0x60 [90.220358] lr : fsl_edma3_terminate_all+0x34/0x20c [90.225237] sp : ffff800013f0bac0 [90.228548] x29: ffff800013f0bac0 x28: 0000000000000001 x27: ffff000008404800 [90.235681] x26: ffff000008404960 x25: ffff000008404a08 x24: ffff000008404a00 [90.242813] x23: ffff000008404a60 x22: 0000000000000002 x21: 0000000000000000 [90.249946] x20: ffff800013f0baf8 x19: ffff00000559c800 x18: 0000000000000000 [90.257078] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [90.264211] x14: 0000000000000003 x13: 0000000000000000 x12: 0000000000000040 [90.271344] x11: ffff00000600c248 x10: ffff800013f0bb10 x9 : ffff000057bcb090 [90.278477] x8 : fffffc0000241a08 x7 : ffff00000534ee00 x6 : ffff000008404804 [90.285609] x5 : 0000000000000000 x4 : 0000000000000000 x3 : ffff0000055b3480 [90.292742] x2 : ffff8000135c0000 x1 : ffff00000534ee00 x0 : ffff00000559c800 [90.299876] Call trace: [90.302321] fsl_edma3_disable_request+0x8/0x60 [90.306851] lpuart_flush_buffer+0x40/0x160 [90.311037] uart_flush_buffer+0x88/0x120 [90.315050] tty_driver_flush_buffer+0x20/0x30 [90.319496] hci_uart_flush+0x44/0x90 [90.323162] +0x34/0x12c [90.327253] tty_ldisc_close+0x38/0x70 [90.331005] tty_ldisc_release+0xa8/0x190 [90.335018] tty_release_struct+0x24/0x8c [90.339022] tty_release+0x3ec/0x4c0 [90.342593] __fput+0x70/0x234 [90.345652] ____fput+0x14/0x20 [90.348790] task_work_run+0x84/0x17c [90.352455] do_exit+0x310/0x96c [90.355688] do_group_exit+0x3c/0xa0 [90.359259] __arm64_sys_exit_group+0x1c/0x20 [90.363609] invoke_syscall+0x48/0x114 [90.367362] el0_svc_common.constprop.0+0xd4/0xfc [90.372068] do_el0_svc+0x2c/0x94 [90.375379] el0_svc+0x28/0x80 [90.378438] el0t_64_sync_handler+0xa8/0x130 [90.382711] el0t_64_sync+0x1a0/0x1a4 [90.386376] Code: 17ffffda d503201f d503233f f9409802 (b9400041) [90.392467] ---[end trace 2f60524b4a43f1f6]--- [90.397073] note: btattach[503] exited with preempt_count 1 [90.402636] Fixing recursive fault but reboot is needed!	N/A	More Details
CVE-2023-53429	In the Linux kernel, the following vulnerability has been resolved: btrfs: don't check PageError in __extent_writepage __extent_writepage currenly sets PageError whenever any error happens, and the also checks for PageError to decide if to call error handling. This leads to very unclear responsibility for cleaning up on errors. In the VM and generic writeback helpers the basic idea is that once I/O is fired off all error handling responsibility is delegated to the end I/O handler. But if that end I/O handler sets the PageError bit, and the submitter checks it, the bit could in some cases leak into the submission context for fast enough I/O. Fix this by simply not checking PageError and just using the local ret variable to check for submission errors. This also fundamentally solves the long problem documented in a comment in __extent_writepage by never leaking the error bit into the submission context.	N/A	More Details
CVE-2022-50376	In the Linux kernel, the following vulnerability has been resolved: orangefs: Fix kmemleak in orangefs_{kernel,client}_debug_init() When insert and remove the orangefs module, there are memory leaked as below: unreferenced object 0xffff88816b0cc000 (size 2048): comm "insmod", pid 783, jiffies 4294813439 (age 65.512s) hex dump (first 32 bytes): 6e 6f 6e 65 0a 00 00 00 00 00 00 00 00 00 00 00 none..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<0000000031ab7788>] kmalloc_trace+0x27/0xa0 [<000000005b405fee>] orangefs_debugfs_init.cold+0xaf/0x17f [<00000000e5a0085b>] 0xffffffffa02780f9 [<000000004232d9f7>] do_one_initcall+0x87/0x2a0 [<0000000054f22384>] do_init_module+0xdf/0x320 [<000000003263bdea>] load_module+0x2f98/0x3330 [<0000000052cd4153>] __do_sys_finit_module+0x113/0x1b0 [<00000000250ae02b>] do_syscall_64+0x35/0x80 [<00000000f11c03c7>] entry_SYSCALL_64_after_hwframe+0x46/0xb0 Use the golbal variable as the buffer rather than dynamic allocate to slove the problem.	N/A	More Details
CVE-2022-50377	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-53428	In the Linux kernel, the following vulnerability has been resolved: powercap: arm_scmi: Remove recursion while parsing zones Powercap zones can be defined as arranged in a hierarchy of trees and when registering a zone with powercap_register_zone(), the kernel powercap subsystem expects this to happen starting from the root zones down to the leaves; on the other side, de-registration by powercap_deregister_zone() must begin from the leaf zones. Available SCMI powercap zones are retrieved dynamically from the platform at probe time and, while any defined hierarchy between the zones is described properly in the zones descriptor, the platform returns the availables zones with no particular well-defined order: as a consequence, the trees possibly composing the hierarchy of zones have to be somehow walked properly to register the retrieved zones from the root. Currently the ARM SCMI Powercap driver walks the zones using a recursive algorithm; this approach, even though correct and tested can lead to kernel stack overflow when processing a returned hierarchy of zones composed by particularly high trees. Avoid possible kernel stack overflow by substituting the recursive approach with an iterative one supported by a dynamically allocated stack-like data structure.	N/A	More Details

CVE-2022-50378	In the Linux kernel, the following vulnerability has been resolved: drm/meson: reorder driver deinit sequence to fix use-after-free bug Unloading the driver triggers the following KASAN warning: [+0.006275] == [+0.000029] BUG: KASAN: use-after-free in __list_del_entry_valid+0xe0/0x1a0 [+0.000026] Read of size 8 at addr ffff000020c395e0 by task rmmod/2695 [+0.000019] CPU: 5 PID: 2695 Comm: rmmod Tainted: G C O 5.19.0-rc6-lrmbkasan+ #1 [+0.000013] Hardware name: Hardkernel ODROID-N2Plus (DT) [+0.000008] Call trace: [+0.000007] dump_backtrace+0x1ec/0x280 [+0.000013] show_stack+0x24/0x80 [+0.000008] dump_stack_lvl+0x98/0xd4 [+0.000011] print_address_description.constprop.0+0x80/0x520 [+0.000011] print_report+0x128/0x260 [+0.000007] kasan_report+0xb8/0xfc [+0.000008] __asan_report_load8_noabort+0x3c/0x50 [+0.000010] __list_del_entry_valid+0xe0/0x1a0 [+0.000009] drm_atomic_private_obj_fini+0x30/0x200 [drm] [+0.000172] drm_bridge_detach+0x94/0x260 [drm] [+0.000145] drm_encoder_cleanup+0xa4/0x290 [drm] [+0.000144] drm_mode_config_cleanup+0x118/0x740 [drm] [+0.000143] drm_mode_config_init_release+0x1c/0x2c [drm] [+0.000144] drm_managed_release+0x170/0x414 [drm] [+0.000142] drm_dev_put.part.0+0xc0/0x124 [drm] [+0.000143] drm_dev_put+0x20/0x30 [drm] [+0.000142] meson_drv_unbind+0x1d8/0x2ac [meson_drm] [+0.000028] take_down_aggregate_device+0xb0/0x160 [+0.000016] component_del+0x18c/0x360 [+0.000009] meson_dw_hdmi_remove+0x28/0x40 [meson_dw_hdmi] [+0.000015] platform_remove+0x64/0xb0 [+0.000009] device_remove+0xb8/0x154 [+0.000009] device_release_driver_internal+0x398/0x5b0 [+0.000009] driver_detach+0xac/0x1b0 [+0.000009] bus_remove_driver+0x158/0x29c [+0.000009] driver_unregister+0x70/0xb0 [+0.000008] platform_driver_unregister+0x20/0x2c [+0.000008] meson_dw_hdmi_platform_driver_exit+0x1c/0x30 [meson_dw_hdmi] [+0.000012] __do_sys_delete_module+0x288/0x400 [+0.000011] __arm64_sys_delete_module+0x5c/0x80 [+0.000009] invoke_syscall+0x74/0x260 [+0.000009] el0_svc_common.constprop.0+0xcc/0x260 [+0.000009] do_el0_svc+0x50/0x70 [+0.000007] el0_svc+0x68/0x1a0 [+0.000012] el0t_64_sync_handler+0x11c/0x150 [+0.000008] el0t_64_sync+0x18c/0x190 [+0.000018] Allocated by task 0: [+0.000007] (stack is not available) [+0.000011] Freed by task 2695: [+0.000008] kasan_save_stack+0x2c/0x5c [+0.000011] kasan_set_track+0x2c/0x40 [+0.000008] kasan_set_free_info+0x28/0x50 [+0.000009] ____kasan_slab_free+0x128/0x1d4 [+0.000008] __kasan_slab_free+0x18/0x24 [+0.000007] slab_free_freelist_hook+0x108/0x230 [+0.000011] kfree+0x110/0x35c [+0.000008] release_nodes+0xf0/0x16c [+0.000009] devres_release_group+0x180/0x270 [+0.000008] component_unbind+0x128/0x1e0 [+0.000010] component_unbind_all+0x1b8/0x264 [+0.000009] meson_drv_unbind+0x1a0/0x2ac [meson_drm] [+0.000025] take_down_aggregate_device+0xb0/0x160 [+0.000009] component_del+0x18c/0x360 [+0.000009] meson_dw_hdmi_remove+0x28/0x40 [meson_dw_hdmi] [+0.000012] platform_remove+0x64/0xb0 [+0.000008] device_remove+0xb8/0x154 [+0.000009] device_release_driver_internal+0x398/0x5b0 [+0.000009] driver_detach+0xac/0x1b0 [+0.000009] bus_remove_driver+0x158/0x29c [+0.000008] driver_unregister+0x70/0xb0 [+0.000008] platform_driver_unregister+0x20/0x2c [+0.000008] meson_dw_hdmi_platform_driver_exit+0x1c/0x30 [meson_dw_hdmi] [+0.000011] __do_sys_delete_module+0x288/0x400 [+0.000010] __arm64_sys_delete_module+0x5c/0x80 [+0.000008] invoke_syscall+0x74/0x260 [+0.000008] el0_svc_common.constprop.0+0xcc/0x260 [+0.000008] do_el0_svc+0x50/0x70 [+0.000007] el0_svc+0x68/0x1a0 [+0.000009] el0t_64_sync_handler+0x11c/0x150 [+0.000009] el0t_64_sync+0x18c/0x190 [+0.000014] The buggy address belongs to the object at ffff000020c39000 ---truncated---	N/A	More Details
CVE-2022-50379	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix race between quota enable and quota rescan ioctl When enabling quotas, at btrfs_quota_enable(), after committing the transaction, we change fs_info->quota_root to point to the quota root we created and set BTRFS_FS_QUOTA_ENABLED at fs_info->flags. Then we try to start the qgroup rescan worker, first by initializing it with a call to qgroup_rescan_init() - however if that fails we end up freeing the quota root but we leave fs_info->quota_root still pointing to it, this can later result in a use-after-free somewhere else. We have previously set the flags BTRFS_FS_QUOTA_ENABLED and BTRFS_QGROUP_STATUS_FLAG_ON, so we can only fail with -EINPROGRESS at btrfs_quota_enable(), which is possible if someone already called the quota rescan ioctl, and therefore started the rescan worker. So fix this by ignoring an -EINPROGRESS and asserting we can't get any other error.	N/A	More Details
CVE-2022-50380	In the Linux kernel, the following vulnerability has been resolved: mm: /proc/pid/smaps_rollup: fix no vma's null-deref Commit 258f669e7e88 ("mm: /proc/pid/smaps_rollup: convert to single value seq_file") introduced a null-deref if there are no vma's in the task in show_smaps_rollup.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: md: fix a crash in mempool_free There's a crash in mempool_free when running the lvm test shell/lvchange-rebuild-raid.sh. The reason for the crash is this: * super_written calls atomic_dec_and_test(&mddev->pending_writes) and wake_up(&mddev->sb_wait). Then it calls rdev_dec_pending(rdev, mddev) and bio_put(bio). * so, the process that waited on sb_wait and that is woken up is racing with bio_put(bio). * if the process wins the race, it calls bioset_exit before bio_put(bio) is executed. * bio_put(bio) attempts to free a bio into a destroyed bio set - causing a crash in mempool_free. We fix this bug by moving bio_put before atomic_dec_and_test. We also move rdev_dec_pending before atomic_dec_and_test as suggested by Neil Brown. The function md_end_flush has a similar bug - we must call bio_put before we decrement the number of in-progress bios. BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor write access in kernel mode #PF:		

CVE-2022-50381	error_code(0x0002) - not-present page PGD 11557f0067 P4D 11557f0067 PUD 0 Oops: 0002 [#1] PREEMPT SMP CPU: 0 PID: 73 Comm: kworker/0:1 Not tainted 6.1.0-rc3 #5 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-2 04/01/2014 Workqueue: kdelayd flush_expired_bios [dm_delay] RIP: 0010:mempool_free+0x47/0x80 Code: 48 89 ef 5b 5d ff e0 f3 c3 48 89 f7 e8 32 45 3f 00 48 63 53 08 48 89 c6 3b 53 04 7d 2d 48 8b 43 10 8d 4a 01 48 89 df 89 4b 08 <48> 89 2c d0 e8 b0 45 3f 00 48 8d 7b 30 5b 5d 31 c9 ba 01 00 00 00 RSP: 0018:ffff88910036bda8 EFLAGS: 00010093 RAX: 0000000000000000 RBX: ffff8891037b65d8 RCX: 0000000000000001 RDX: 0000000000000000 RSI: 0000000000000202 RDI: ffff8891037b65d8 RBP: ffff8891447ba240 R08: 0000000000012908 R09: 00000000003d0900 R10: 0000000000000000 R11: 0000000000173544 R12: ffff889101a14000 R13: ffff8891562ac300 R14: ffff889102b41440 R15: ffffe8ffffa00d05 FS: 0000000000000000(0000) GS:ffff88942fa00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 0000001102e99000 CR4: 00000000000006b0 Call Trace: <TASK> clone_endio+0xf4/0x1c0 [dm_mod] clone_endio+0xf4/0x1c0 [dm_mod] __submit_bio+0x76/0x120 submit_bio_noacct_nocheck+0xb6/0x2a0 flush_expired_bios+0x28/0x2f [dm_delay] process_one_work+0x1b4/0x300 worker_thread+0x45/0x3e0 ? rescuer_thread+0x380/0x380 kthread+0xc2/0x100 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x1f/0x30 </TASK> Modules linked in: brd dm_delay dm_raid dm_mod af_packet uvesafb cfbfillrect cfbimgblt cn cfbcopyarea fb font fbdev tun autofs4 binfmt_misc configfs ipv6 virtio_rng virtio_balloon rng_core virtio_net pcspkr net_failover failover qemu_fw_cfg button mousedev raid10 raid456 libcrc32c async_raid6_recov async_memcpy async_pq raid6_pq async_xor xor async_tx raid1 raid0 md_mod sd_mod t10_pi crc64_rocksoft crc64 virtio_scsi scsi_mod evdev psmouse bsg scsi_common [last unloaded: brd] CR2: 0000000000000000 ---[end trace 0000000000000000]---	N/A	More Details
CVE-2022-50382	In the Linux kernel, the following vulnerability has been resolved: padata: Always leave BHs disabled when running ->parallel() A deadlock can happen when an overloaded system runs ->parallel() in the context of the current task: padata_do_parallel ->parallel() pcrypt_aead_enc/dec padata_do_serial spin_lock(&reorder->lock) // BHs still enabled <interrupt> ... __do_softirq ... padata_do_serial spin_lock(&reorder->lock) It's a bug for BHs to be on in _do_serial as Steffen points out, so ensure they're off in the "current task" case like they are in padata_parallel_worker to avoid this situation.	N/A	More Details
CVE-2022-50383	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: Can't set dst buffer to done when lat decode error Core thread will call v4l2_m2m_buf_done to set dst buffer done for lat architecture. If lat call v4l2_m2m_buf_done_and_job_finish to free dst buffer when lat decode error, core thread will access kernel NULL pointer dereference, then crash.	N/A	More Details
CVE-2023-53437	In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Handle cameras with invalid descriptors If the source entity does not contain any pads, do not create a link.	N/A	More Details
CVE-2025-6237	A vulnerability in invokeai version v6.0.0a1 and below allows attackers to perform path traversal and arbitrary file deletion via the GET /api/v1/images/download/{bulk_download_item_name} endpoint. By manipulating the filename arguments, attackers can read and delete any files on the server, including critical system files such as SSH keys, databases, and configuration files. This vulnerability results in high confidentiality, integrity, and availability impacts.	N/A	More Details
CVE-2025-7993	Ashlar-Vellum Cobalt LI File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of LI files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25355.	N/A	More Details
CVE-2023-53439	In the Linux kernel, the following vulnerability has been resolved: net: skb_partial_csum_set() fix against transport header magic value skb->transport_header uses the special 0xFFFF value to mark if the transport header was set or not. We must prevent callers to accidentaly set skb->transport_header to 0xFFFF. Note that only fuzzers can possibly do this today. syzbot reported: WARNING: CPU: 0 PID: 2340 at include/linux/skbuff.h:2847 skb_transport_offset include/linux/skbuff.h:2956 [inline] WARNING: CPU: 0 PID: 2340 at include/linux/skbuff.h:2847 virtio_net_hdr_to_skb+0xbcc/0x10c0 include/linux/virtio_net.h:103 Modules linked in: CPU: 0 PID: 2340 Comm: syz-executor.0 Not tainted 6.3.0-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/14/2023 RIP: 0010:skb_transport_header include/linux/skbuff.h:2847 [inline] RIP: 0010:skb_transport_offset include/linux/skbuff.h:2956 [inline] RIP: 0010:virtio_net_hdr_to_skb+0xbcc/0x10c0 include/linux/virtio_net.h:103 Code: 41 39 df 0f 82 c3 04 00 00 48 8b 7c 24 10 44 89 e6 e8 08 6e 59 ff 48 85 c0 74 54 e8 ce 36 7e fc e9 37 f8 ff ff e8 c4 36 7e fc <0f> 0b e9 93 f8 ff ff 44 89 f7 44 89 e6 e8 32 38 7e fc 45 39 e6 0f RSP: 0018:ffffc90004497880 EFLAGS: 00010293 RAX: ffffffff84fea55c RBX: 000000000000ffff RCX: ffff888120be2100 RDX: 0000000000000000 RSI: 000000000000ffff RDI: 000000000000ffff RBP: ffffc90004497990 R08: ffffffff84fe9de5 R09: 0000000000000034 R10: ffffea00048ebd80 R11: 0000000000000034 R12: ffff88811dc2d9c8 R13: dfffffc0000000000 R14: ffff88811dc2d9ae R15: 1ffff11023b85b35 FS: 00007f9211a59700(0000) GS:ffff8881f6c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000200002c0 CR3: 00000001215a5000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> packet_snd	N/A	More Details

	net/packet/af_packet.c:3076 [inline] packet_sendmsg+0x4590/0x61a0 net/packet/af_packet.c:3115 sock_sendmsg_nosec net/socket.c:724 [inline] sock_sendmsg net/socket.c:747 [inline] __sys_sendto+0x472/0x630 net/socket.c:2144 __do_sys_sendto net/socket.c:2156 [inline] __se_sys_sendto net/socket.c:2152 [inline] __x64_sys_sendto+0xe5/0x100 net/socket.c:2152 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x2f/0x50 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7f9210c8c169 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 f1 19 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f9211a59168 EFLAGS: 00000246 ORIG_RAX: 000000000000002c RAX: ffffffffffffffda RBX: 00007f9210dabf80 RCX: 00007f9210c8c169 RDX: 000000000000ffed RSI: 00000000200000c0 RDI: 0000000000000003 RBP: 00007f9210ce7ca1 R08: 0000000020000540 R09: 0000000000000014 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007ffe135d65cf R14: 00007f9211a59300 R15: 0000000000022000		
CVE-2023-53446	In the Linux kernel, the following vulnerability has been resolved: PCI/ASPM: Disable ASPM on MFD function removal to avoid use-after-free Struct pcie_link_state->downstream is a pointer to the pci_dev of function 0. Previously we retained that pointer when removing function 0, and subsequent ASPM policy changes dereferenced it, resulting in a use-after-free warning from KASAN, e.g.: # echo 1 > /sys/bus/pci/devices/0000:03:00.0/remove # echo powersave > /sys/module/pcie_aspm/parameters/policy BUG: KASAN: slab-use-after-free in pcie_config_aspm_link+0x42d/0x500 Call Trace: kasan_report+0xae/0xe0 pcie_config_aspm_link+0x42d/0x500 pcie_aspm_set_policy+0x8e/0x1a0 param_attr_store+0x162/0x2c0 module_attr_store+0x3e/0x80 PCIe spec r6.0, sec 7.5.3.7, recommends that software program the same ASPM Control value in all functions of multi-function devices. Disable ASPM and free the pcie_link_state when any child function is removed so we can discard the dangling pcie_link_state->downstream pointer and maintain the same ASPM Control configuration for all functions. [bhelgaas: commit log and comment]	N/A	More Details
CVE-2025-7994	Ashlar-Vellum Cobalt AR File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25976.	N/A	More Details
CVE-2025-7995	Ashlar-Vellum Cobalt CO File Parsing Type Confusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25981.	N/A	More Details
CVE-2025-7996	Ashlar-Vellum Cobalt AR File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25982.	N/A	More Details
CVE-2025-7997	Ashlar-Vellum Cobalt XE File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of proper validation of user-supplied data, which can result in a read before the start of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26045.	N/A	More Details
CVE-2023-53445	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: Fix a refcount bug in qrtr_recvmsg() Syzbot reported a bug as following: refcount_t: addition on 0; use-after-free. ... RIP: 0010:refcount_warn_saturate+0x17c/0x1f0 lib/refcount.c:25 ... Call Trace: <TASK> __refcount_add include/linux/refcount.h:199 [inline] __refcount_inc include/linux/refcount.h:250 [inline] refcount_inc include/linux/refcount.h:267 [inline] kref_get include/linux/kref.h:45 [inline] qrtr_node_acquire net/qrtr/af_qrtr.c:202 [inline] qrtr_node_lookup net/qrtr/af_qrtr.c:398 [inline] qrtr_send_resume_tx net/qrtr/af_qrtr.c:1003 [inline] qrtr_recvmsg+0x85f/0x990 net/qrtr/af_qrtr.c:1070 sock_recvmsg_nosec net/socket.c:1017 [inline] sock_recvmsg+0xe2/0x160 net/socket.c:1038 qrtr_ns_worker+0x170/0x1700 net/qrtr/ns.c:688 process_one_work+0x991/0x15c0 kernel/workqueue.c:2390 worker_thread+0x669/0x1090 kernel/workqueue.c:2537 It occurs in the concurrent scenario of qrtr_recvmsg() and qrtr_endpoint_unregister() as following: cpu0 cpu1 qrtr_recvmsg qrtr_endpoint_unregister qrtr_send_resume_tx qrtr_node_release qrtr_node_lookup mutex_lock(&qrtr_node_lock) spin_lock_irqsave(&qrtr_nodes_lock,) refcount_dec_and_test(&node->ref) [node->ref == 0] radix_tree_lookup [node != NULL] __qrtr_node_release qrtr_node_acquire spin_lock_irqsave(&qrtr_nodes_lock,	N/A	More Details

	) kref_get(&node->ref) [WARNING] ... mutex_unlock(&qrtr_node_lock) Use qrtr_node_lock to protect qrtr_node_lookup() implementation, this is actually improving the protection of node reference.		
CVE-2023-53444	In the Linux kernel, the following vulnerability has been resolved: drm/ttm: fix bulk_move corruption when adding a entry When the resource is the first in the bulk_move range, adding it again (thus moving it to the tail) will corrupt the list since the first pointer is not moved. This eventually lead to null pointer deref in ttm_lru_bulk_move_del()	N/A	More Details
CVE-2025-7998	Ashlar-Vellum Cobalt CO File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26046.	N/A	More Details
CVE-2025-9983	GALAYOU G2 cameras stream video output via RTSP streams. By default these streams are protected by randomly generated credentials. However these credentials are not required to access the stream. Changing these values does not change camera's behavior. The vendor did not respond in any way. Only version 11.100001.01.28 was tested, other versions might also be vulnerable.	N/A	More Details
CVE-2025-7999	Ashlar-Vellum Cobalt AR File Parsing Type Confusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AR files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26049.	N/A	More Details
CVE-2023-53443	In the Linux kernel, the following vulnerability has been resolved: mfd: arizona: Use pm_runtime_resume_and_get() to prevent refcnt leak In arizona_clk32k_enable(), we should use pm_runtime_resume_and_get() as pm_runtime_get_sync() will increase the refcnt even when it returns an error.	N/A	More Details
CVE-2025-8000	Ashlar-Vellum Cobalt LI File Parsing Type Confusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of LI files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26051.	N/A	More Details
CVE-2025-8001	Ashlar-Vellum Cobalt CO File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26053.	N/A	More Details
CVE-2025-8002	Ashlar-Vellum Cobalt CO File Parsing Type Confusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26233.	N/A	More Details
CVE-2025-8003	Ashlar-Vellum Cobalt CO File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26235.	N/A	More Details
CVE-2025-8004	Ashlar-Vellum Cobalt XE File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26236.	N/A	More Details
	Ashlar-Vellum Cobalt XE File Parsing Type Confusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User		

CVE-2025-8005	interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26237.	N/A	More Details
CVE-2025-8006	Ashlar-Vellum Cobalt XE File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26238.	N/A	More Details
CVE-2023-53442	In the Linux kernel, the following vulnerability has been resolved: ice: Block switchdev mode when ADQ is active and vice versa ADQ and switchdev are not supported simultaneously. Enabling both at the same time can result in nullptr dereference. To prevent this, check if ADQ is active when changing devlink mode to switchdev mode, and check if switchdev is active when enabling ADQ.	N/A	More Details
CVE-2023-53441	In the Linux kernel, the following vulnerability has been resolved: bpf: cpumap: Fix memory leak in cpu_map_update_elem Syzkaller reported a memory leak as follows: BUG: memory leak unreferenced object 0xff110001198ef748 (size 192): comm "syz-executor.3", pid 17672, jiffies 4298118891 (age 9.906s) hex dump (first 32 bytes): 00 00 00 00 4a 19 00 00 80 ad e3 e4 fe ff c0 00 ....J..... 00 b2 d3 0c 01 00 11 ff 28 f5 8e 19 01 00 11 ff ....(..... backtrace: [<ffffffffadd28087>] __cpu_map_entry_alloc+0xf7/0xb00 [<ffffffffadd28d8e>] cpu_map_update_elem+0x2fe/0x3d0 [<ffffffffadc6d0fd>] bpf_map_update_value.isra.0+0x2bd/0x520 [<ffffffffadc7349b>] map_update_elem+0x4cb/0x720 [<ffffffffadc7d983>] __se_sys_bpf+0x8c3/0xb90 [<ffffffffb029cc80>] do_syscall_64+0x30/0x40 [<ffffffffb0400099>] entry_SYSCALL_64_after_hwframe+0x61/0xc6 BUG: memory leak unreferenced object 0xff110001198ef528 (size 192): comm "syz-executor.3", pid 17672, jiffies 4298118891 (age 9.906s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<ffffffffadd281f0>] __cpu_map_entry_alloc+0x260/0xb00 [<ffffffffadd28d8e>] cpu_map_update_elem+0x2fe/0x3d0 [<ffffffffadc6d0fd>] bpf_map_update_value.isra.0+0x2bd/0x520 [<ffffffffadc7349b>] map_update_elem+0x4cb/0x720 [<ffffffffadc7d983>] __se_sys_bpf+0x8c3/0xb90 [<ffffffffb029cc80>] do_syscall_64+0x30/0x40 [<ffffffffb0400099>] entry_SYSCALL_64_after_hwframe+0x61/0xc6 BUG: memory leak unreferenced object 0xff1100010fd93d68 (size 8): comm "syz-executor.3", pid 17672, jiffies 4298118891 (age 9.906s) hex dump (first 8 bytes): 00 00 00 00 00 00 00 00 .... backtrace: [<ffffffffade5db3e>] kvmalloc_node+0x11e/0x170 [<ffffffffadd28280>] __cpu_map_entry_alloc+0x2f0/0xb00 [<ffffffffadd28d8e>] cpu_map_update_elem+0x2fe/0x3d0 [<ffffffffadc6d0fd>] bpf_map_update_value.isra.0+0x2bd/0x520 [<ffffffffadc7349b>] map_update_elem+0x4cb/0x720 [<ffffffffadc7d983>] __se_sys_bpf+0x8c3/0xb90 [<ffffffffb029cc80>] do_syscall_64+0x30/0x40 [<ffffffffb0400099>] entry_SYSCALL_64_after_hwframe+0x61/0xc6 In the cpu_map_update_elem flow, when kthread_stop is called before calling the threadfn of rcpu->kthread, since the KTHREAD_SHOULD_STOP bit of kthread has been set by kthread_stop, the threadfn of rcpu->kthread will never be executed, and rcpu->refcnt will never be 0, which will lead to the allocated rcpu, rcpu->queue and rcpu->queue->queue cannot be released. Calling kthread_stop before executing kthread's threadfn will return -EINTR. We can complete the release of memory resources in this state.	N/A	More Details
CVE-2023-53440	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix sysfs interface lifetime The current nilfs2 sysfs support has issues with the timing of creation and deletion of sysfs entries, potentially leading to null pointer dereferences, use-after-free, and lockdep warnings. Some of the sysfs attributes for nilfs2 per-filesystem instance refer to metadata file "cpfile", "sufile", or "dat", but nilfs_sysfs_create_device_group that creates those attributes is executed before the inodes for these metadata files are loaded, and nilfs_sysfs_delete_device_group which deletes these sysfs entries is called after releasing their metadata file inodes. Therefore, access to some of these sysfs attributes may occur outside of the lifetime of these metadata files, resulting in inode NULL pointer dereferences or use-after-free. In addition, the call to nilfs_sysfs_create_device_group() is made during the locking period of the semaphore "ns_sem" of nilfs object, so the shrinker call caused by the memory allocation for the sysfs entries, may derive lock dependencies "ns_sem" -> (shrinker) -> "locks acquired in nilfs_evict_inode()". Since nilfs2 may acquire "ns_sem" deep in the call stack holding other locks via its error handler __nilfs_error(), this causes lockdep to report circular locking. This is a false positive and no circular locking actually occurs as no inodes exist yet when nilfs_sysfs_create_device_group() is called. Fortunately, the lockdep warnings can be resolved by simply moving the call to nilfs_sysfs_create_device_group() out of "ns_sem". This fixes these sysfs issues by revising where the device's sysfs interface is created/deleted and keeping its lifetime within the lifetime of the metadata files above.	N/A	More Details
CVE-2025-39848	In the Linux kernel, the following vulnerability has been resolved: ax25: properly unshare skbs in ax25_kiss_rcv() Bernard Pidoux reported a regression apparently caused by commit c353e8983e0d ("net: introduce per netns packet chains"). skb->dev becomes NULL and we crash in __netif_receive_skb_core(). Before above commit, different kind of bugs or corruptions could happen without a major crash. But the root cause is that ax25_kiss_rcv() can queue/mangle input skb without checking if this skb is shared or not. Many	N/A	More Details

	thanks to Bernard Pidoux for his help, diagnosis and tests. We had a similar issue years ago fixed with commit 7aaed57c5c28 ("phonet: properly unshare skbs in phonet_rcv()").		