SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 December 2025

Generated on 10 December 2025

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-13390	The WP Directory Kit plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 1.4.4 due to incorrect implementation of the authentication algorithm in the "wdk_generate_auto_login_link" function. This is due to the feature using a cryptographically weak token generation mechanism. This makes it possible for unauthenticated attackers to gain administrative access and achieve full site takeover via the auto-login endpoint with a predictable token.	10.0	More Details
CVE-2025-55182	A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.	10.0	More Details
CVE-2025-66570	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.27.0, a vulnerability allows attacker-controlled HTTP headers to influence server-visible metadata, logging, and authorization decisions. An attacker can inject headers named REMOTE_ADDR, REMOTE_PORT, LOCAL_ADDR, LOCAL_PORT that are parsed into the request header multimap via read_headers() in httplib.h (headers.emplace), then the server later appends its own internal metadata using the same header names in Server::process_request without erasing duplicates. Because Request::get_header_value returns the first entry for a header key (id == 0) and the client-supplied headers are parsed before server-inserted headers, downstream code that uses these header names may inadvertently use attacker-controlled values. Affected files/locations: cpp-httplib/httplib.h (read_headers, Server::process_request, Request::get_header_value, get_header_value_u64) and cpp-httplib/docker/main.cc (get_client_ip, nginx_access_logger, nginx_error_logger). Attack surface: attacker-controlled HTTP headers in incoming requests flow into the Request.headers multimap and into logging code that reads forwarded headers, enabling IP spoofing, log poisoning, and authorization bypass via header shadowing. This vulnerability is fixed in 0.27.0.	10.0	More Details
CVE-2025-42880	Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system.	9.9	More Details
CVE-2025-13486	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Remote Code Execution in versions 0.9.0.5 through 0.9.1.1 via the prepare_form() function. This is due to the function accepting user input and then passing that through call_user_func_array(). This makes it possible for unauthenticated attackers to execute arbitrary code on the server, which can be leveraged to inject backdoors or create new administrative user accounts.	9.8	More Details
CVE-2025-48626	In multiple locations, there is a possible way to launch an application from the background due to a precondition check failure. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2025-13342	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to unauthorized modification of arbitrary WordPress options in all versions up to, and including, 3.28.20. This is due to insufficient capability checks and input validation in the ActionOptions::run() save handler. This makes it possible for unauthenticated attackers to modify critical WordPress options such as users_can_register, default_role, and admin_email via submitting crafted form data to public frontend forms.	9.8	More Details
CVE-2025-12673	The Flex QR Code Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the update_qr_code() function in all versions up to, and including, 1.2.6. 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-2025-27019	Remote shell service (RSH) in Infinera MTC-9 version R22.1.1.0275 allows an attacker to utilize password-less user accounts and obtain system access by activating a reverse shell.This issue affects MTC-9: from R22.1.1.0275 before R23.0.	9.8	More Details
CVE-2025-27020	Improper configuration of the SSH service in Infinera MTC-9 allows an unauthenticated attacker to execute arbitrary commands and access data on file system . This issue affects MTC-9: from R22.1.1.0275 before R23.0.	9.8	More Details
CVE-2025-12504	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TalentSoft Software UNIS allows SQL Injection.This issue affects UNIS: before 42321.	9.8	More Details

CVE-2025-64081	SQL injection vulnerability in /php/api_patient_schedule.php in SourceCodester Patients Waiting Area Queue Management System v1 allows attackers to execute arbitrary SQL commands via the appointmentID parameter.	9.8	More Details
CVE-2025-29269	ALLNET ALL-RUT22GW v3.3.8 was discovered to contain an OS command injection vulnerability via the command parameter in the popen.cgi endpoint.	9.8	More Details
CVE-2025-59718	A improper verification of cryptographic signature vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0.0 through 7.0.21, FortiSwitchManager 7.2.0 through 7.2.6, FortiSwitchManager 7.0.0 through 7.0.5 allows an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML response message.	9.8	More Details
CVE-2025-59719	An improper verification of cryptographic signature vulnerability in Fortinet FortiWeb 8.0.0, FortiWeb 7.6.0 through 7.6.4, FortiWeb 7.4.0 through 7.4.9 may allow an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML response message.	9.8	More Details
CVE-2025-67489	@vitejs/plugin-rs provides React Server Components (RSC) support for Vite. Versions 0.5.5 and below are vulnerable to arbitrary remote code execution on the development server through unsafe dynamic imports in server function APIs (loadServerAction, decodeReply, decodeAction) when integrated into RSC applications that expose server function endpoints. Attackers with network access to the development server can read/modify files, exfiltrate sensitive data (source code, environment variables, credentials), or pivot to other internal services. While this affects development servers only, the risk increases when using vite --host to expose the server on all network interfaces. This issue is fixed in version 0.5.6.	9.8	More Details
CVE-2025-13313	The CRM Memberships plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, and including, 2.5. This is due to missing authorization and authentication checks on the `ntzcrm_changepassword` AJAX action. This makes it possible for unauthenticated attackers to reset arbitrary user passwords and gain unauthorized access to user accounts via the `ntzcrm_changepassword` endpoint, granted they can obtain or enumerate a target user's email address. The plugin also exposes the `ntzcrm_get_users` endpoint without authentication, allowing attackers to enumerate subscriber email addresses, facilitating the exploitation of the password reset vulnerability.	9.8	More Details
CVE-2025-12374	The Email Verification, Email OTP, Block Spam Email, Passwordless login, Hide Login, Magic Login – User Verification plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.39. This is due to the plugin not properly validating that an OTP was generated before comparing it to user input in the "user_verification_form_wrap_process_otpLogin" function. This makes it possible for unauthenticated attackers to log in as any user with a verified email address, such as an administrator, by submitting an empty OTP value.	9.8	More Details
CVE-2025-29268	ALLNET ALL-RUT22GW v3.3.8 was discovered to store hardcoded credentials in the libicos.so library.	9.8	More Details
CVE-2025-53963	An issue was discovered on Thermo Fisher Ion Torrent OneTouch 2 INS1005527 devices. They run an SSH server accessible over the default port 22. The root account has a weak default password of ionadmin, and a password change policy for the root account is not enforced. Thus, an attacker with network connectivity can achieve root code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2024-32641	Masa CMS is an open source Enterprise Content Management platform. Masa CMS versions prior to 7.2.8, 7.3.13, and 7.4.6 are vulnerable to remote code execution. The vulnerability exists in the addParam function, which accepts user input via the criteria parameter. This input is subsequently evaluated by setDynamicContent, allowing an unauthenticated attacker to execute arbitrary code via the m tag. The vulnerability is patched in versions 7.2.8, 7.3.13, and 7.4.6.	9.8	More Details
CVE-2025-66032	Claude Code is an agentic coding tool. Prior to 1.0.93, Due to errors in parsing shell commands related to $IFS and short CLI flags, it was possible to bypass the Claude Code read-only validation and trigger arbitrary code execution. Reliably exploiting this requires the ability to add untrusted content into a Claude Code context window. This vulnerability is fixed in 1.0.93.	9.8	More Details
CVE-2025-66208	Collabora Online - Built-in CODE Server (richdocumentscode) provides a built-in server with all of the document editing features of Collabora Online. In versions prior to 25.04.702, Collabora Online has a Configuration-Dependent RCE (OS Command Injection) in richdocumentscode proxy. Users of Nextcloud with Collabora Online - Built-in CODE Server app can be vulnerable to attack via proxy.php and an intermediate reverse proxy. This vulnerability is fixed in 25.04.702.	9.8	More Details
CVE-2025-63362	Waveshare RS232/485 TO WIFI ETH (B) Serial to Ethernet/Wi-Fi Gateway Firmware V3.1.1.0: HW 4.3.2.1: Webpage V7.04T.07.002880.0301 allows attackers to set the Administrator password and username as blank values, allowing attackers to bypass authentication.	9.8	More Details
CVE-2025-64055	An issue was discovered in Fanvil x210 V2 2.12.20 allowing unauthenticated attackers on the local network to access administrative functions of the device (e.g. file upload, firmware update, reboot...) via a crafted authentication bypass.	9.8	More Details
CVE-2025-54303	The Thermo Fisher Torrent Suite Django application 5.18.1 has weak default credentials, which are stored as fixtures for the Django ORM API. The ionadmin user account can be used to authenticate to default deployments with the password ionadmin. The user guide recommends changing default credentials; however, a password change policy for default administrative accounts is not enforced. Many deployments may retain default credentials, in which case an attacker is likely to be able to successfully authenticate with administrative privileges.	9.8	More Details
CVE-2025-54304	An issue was discovered on Thermo Fisher Ion Torrent OneTouch 2 INS1005527 devices. When they are powered on, an X11 display server is started. The display server listens on all network interfaces and is accessible over port 6000. The X11 access control list, by default, allows connections from 127.0.0.1 and 192.168.2.15. If a device is powered on and later connected to a network with DHCP, the device may not be assigned the 192.168.2.15 IP address, leaving the display server accessible by other devices on the network. The exposed X11 display server can then be used to gain root privileges and the ability to execute code remotely by interacting with matchbox-desktop and spawning a terminal. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2025-13377	The 10Web Booster – Website speed optimization, Cache & Page Speed optimizer plugin for WordPress is vulnerable to arbitrary folder deletion due to insufficient file path validation in the get_cache_dir_for_page_from_url() function in all versions up to, and including, 2.32.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary folders on the server, which can easily lead to a loss of data or a denial of service condition.	9.6	More Details
CVE-2024-45538	Cross-Site Request Forgery (CSRF) vulnerability in WebAPI Framework in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 and 7.2.2-72806 and Synology Unified Controller (DSMUC) before 3.1.4-23079 allows remote attackers to execute arbitrary code via unspecified vectors.	9.6	More Details

CVE-2025-66481	DeepChat is an open-source AI chat platform that supports cloud models and LLMs. Versions 0.5.1 and below are vulnerable to XSS attacks through improperly sanitized Mermaid content. The recent security patch for MermaidArtifact.vue is insufficient and can be bypassed using unquoted HTML attributes combined with HTML entity encoding. Remote Code Execution is possible on the victim's machine via the electron.ipcRenderer interface, bypassing the regex filter intended to strip dangerous attributes. There is no fix at time of publication.	9.6	More Details
CVE-2025-10573	Stored XSS in Ivanti Endpoint Manager prior to version 2024 SU4 SR1 allows a remote unauthenticated attacker to execute arbitrary JavaScript in the context of an administrator session. User interaction is required.	9.6	More Details
CVE-2025-11022	Cross-Site Request Forgery (CSRF) vulnerability in Personal Project Panilux allows Cross Site Request Forgery. This CSRF vulnerability resulting in Command Injection has been identified. This issue affects Panilux: before v.0.10.0. NOTE: The vendor was contacted and responded that they deny ownership of the mentioned product.	9.6	More Details
CVE-2025-66222	DeepChat is a smart assistant uses artificial intelligence. In 0.5.0 and earlier, there is a Stored Cross-Site Scripting (XSS) vulnerability in the Mermaid diagram renderer allows an attacker to execute arbitrary JavaScript within the application context. By leveraging the exposed Electron IPC bridge, this XSS can be escalated to Remote Code Execution (RCE) by registering and starting a malicious MCP (Model Context Protocol) server.	9.6	More Details
CVE-2025-64054	A reflected Cross Site Scripting (XSS) vulnerability on Fanvil x210 2.12.20 devices allows attackers to cause a denial of service or potentially execute arbitrary commands via crafted POST request to the /cgi-bin/webconfig?page=upload&action=submit endpoint.	9.6	More Details
CVE-2025-67494	ZITADEL is an open-source identity infrastructure tool. Versions 4.7.0 and below are vulnerable to an unauthenticated, full-read SSRF vulnerability. The ZITADEL Login UI (V2) treats the x-zitadel-forward-host header as a trusted fallback for all deployments, including self-hosted instances. This allows an unauthenticated attacker to force the server to make HTTP requests to arbitrary domains, such as internal addresses, and read the responses, enabling data exfiltration and bypassing network-segmentation controls. This issue is fixed in version 4.7.1.	9.3	More Details
CVE-2025-61318	Emlog Pro 2.5.20 has an arbitrary file deletion vulnerability. This vulnerability stems from the admin/template.php component and the admin/plugin.php component. They fail to perform path verification and dangerous code filtering for deletion parameters, allowing attackers to exploit this feature for directory traversal.	9.1	More Details
CVE-2025-65868	XML external entity (XXE) injection in eyoucms v1.7.1 allows remote attackers to cause a denial of service via crafted body of a POST request.	9.1	More Details
CVE-2025-42928	Under certain conditions, a high privileged user could exploit a deserialization vulnerability in SAP jConnect to launch remote code execution. The system may be vulnerable when specially crafted input is used to exploit the vulnerability resulting in high impact on confidentiality, integrity and availability of the system.	9.1	More Details
CVE-2025-67504	WBCE CMS is a content management system. Versions 1.6.4 and below use function GenerateRandomPassword() to create passwords using PHP's rand(). rand() is not cryptographically secure, which allows password sequences to be predicted or brute-forced. This can lead to user account compromise or privilege escalation if these passwords are used for new accounts or password resets. The vulnerability is fixed in version 1.6.5.	9.1	More Details
CVE-2025-65346	alexusmai laravel-file-manager 3.3.1 and below is vulnerable to Directory Traversal. The unzip/extraction functionality improperly allows archive contents to be written to arbitrary locations on the filesystem due to insufficient validation of extraction paths.	9.1	More Details
CVE-2025-65267	In ERPNext v15.83.2 and Frappe Framework v15.86.0, improper validation of uploaded SVG avatar images allows attackers to embed malicious JavaScript. The payload executes when an administrator clicks the image link to view the avatar, resulting in stored cross-site scripting (XSS). Successful exploitation may lead to account takeover, privilege escalation, or full compromise of the affected ERPNext instance.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-14015	A weakness has been identified in H3C Magic B0 up to 100R002. This impacts the function EditWlanMacList of the file /goform/aspForm. This manipulation of the argument param causes buffer overflow. Remote exploitation of the attack is possible. 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-2025-57201	AVTECH SECURITY Corporation DGM1104 FullImg-1015-1004-1006-1003 was discovered to contain an authenticated command injection vulnerability in the SMB server function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	8.8	More Details
CVE-2024-32642	Masa CMS is an open source Enterprise Content Management platform. Prior to 7.2.8, 7.3.13, and 7.4.6, there is vulnerable to host header poisoning which allows account takeover via password reset email. This vulnerability is fixed in 7.2.8, 7.3.13, and 7.4.6.	8.8	More Details
CVE-2025-14196	A weakness has been identified in H3C Magic B1 up to 100R004. The affected element is the function sub_44de0 of the file /goform/aspForm. This manipulation of the argument param causes buffer overflow. Remote exploitation of the attack is possible. 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-2025-64672	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	8.8	More Details
CVE-2025-13543	The PostGallery plugin for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the 'PostGalleryUploader' class functions in all versions up to, and including, 1.12.5. This makes it possible for authenticated attackers, with subscriber-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-65897	zdh_web is a data collection, processing, monitoring, scheduling, and management platform. In zdh_web thru 5.6.17, insufficient validation of file upload paths in the application allows an authenticated user to write arbitrary files to the server file system, potentially overwriting existing files and leading to privilege escalation or remote code execution.	8.8	More Details

CVE-2025-65730	Authentication Bypass via Hardcoded Credentials GoAway up to v0.62.18, fixed in 0.62.19, uses a hardcoded secret for signing JWT tokens used for authentication.	8.8	More Details
CVE-2025-14329	Privilege escalation in the Netmonitor component. This vulnerability affects Firefox < 146 and Firefox ESR < 140.6.	8.8	More Details
CVE-2025-14328	Privilege escalation in the Netmonitor component. This vulnerability affects Firefox < 146 and Firefox ESR < 140.6.	8.8	More Details
CVE-2025-13659	Improper control of dynamically managed code resources in Ivanti Endpoint Manager prior to version 2024 SU4 SR1 allows a remote, unauthenticated attacker to write arbitrary files on the server, potentially leading to remote code execution. User interaction is required.	8.8	More Details
CVE-2024-56835	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). The DHCP Server configuration file of the affected products is subject to code injection. An attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.	8.8	More Details
CVE-2025-13066	The Demo Importer Plus plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 2.0.6. This is due to insufficient file type validation detecting WXR files, allowing double extension files to bypass sanitization while being accepted as a valid WXR file. This makes it possible for authenticated attackers, with author-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-2025-33208	NVIDIA TAO contains a vulnerability where an attacker may cause a resource to be loaded via an uncontrolled search path. A successful exploit of this vulnerability may lead to escalation of privileges, data tampering, denial of service, information disclosure.	8.8	More Details
CVE-2025-12879	The User Generator and Importer plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.2.2. This is due to missing nonce validation in the "Import Using CSV File" function. This makes it possible for unauthenticated attackers to elevate user privileges by creating arbitrary accounts with administrator privileges via a forged request, provided they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2025-62550	Out-of-bounds write in Azure Monitor Agent allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2025-62549	Untrusted pointer dereference in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-12153	The Featured Image via URL plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation function in all versions up to, and including, 0.1. This makes it possible for authenticated attackers, with Contributor-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-2025-12154	The Auto Thumbnailer plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the uploadThumb() function in all versions up to, and including, 1.0. This makes it possible for authenticated attackers, with Contributor-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-2025-33213	NVIDIA Merlin Transformers4Rec for Linux contains a vulnerability in the Trainer component, where a user could cause a deserialization issue. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	8.8	More Details
CVE-2025-33214	NVIDIA NVTabular for Linux contains a vulnerability in the Workflow component, where a user could cause a deserialization issue. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, and data tampering.	8.8	More Details
CVE-2025-12181	The ContentStudio plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the cstu_update_post() function in all versions up to, and including, 1.3.7. This makes it possible for authenticated attackers, with Author-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-2025-62456	Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2025-54307	An issue was discovered in the Thermo Fisher Torrent Suite Django application 5.18.1. The /configure/plugins/plugin/upload/zip/ and /configure/newupdates/offline/bundle/upload/ endpoints allow low-privilege users to upload ZIP files to the server. The plupload_file_upload function handles these file uploads and constructs the destination file path by using either the name parameter or the uploaded filename, neither of which is properly sanitized. The file extension is extracted by splitting the filename, and a format string is used to construct the final file path, leaving the destination path vulnerable to path traversal. An authenticated attacker with network connectivity can write arbitrary files to the server, enabling remote code execution after overwriting an executable file. An example is the pdflatex executable, which is executed through subprocess.Popen in the write_report_pdf function after requests to a /report/latex/(\d+).pdf endpoint.	8.8	More Details
CVE-2025-60024	Multiple Improper Limitations of a Pathname to a Restricted Directory ('Path Traversal') vulnerabilities [CWE-22] vulnerability in Fortinet FortiVoice 7.2.0 through 7.2.2, FortiVoice 7.0.0 through 7.0.7 may allow a privileged authenticated attacker to write arbitrary files via specifically HTTP or HTTPS commands	8.8	More Details
CVE-2025-14191	A vulnerability has been found in UTT 进取 512W up to 1.7.7-171114. Affected by this issue is the function strcpy of the file /goform/formP2PLimitConfig. Such manipulation of the argument except leads to buffer overflow. It is possible to launch the attack 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.	8.8	More Details
CVE-2025-14323	Privilege escalation in the DOM: Notifications component. This vulnerability affects Firefox < 146, Firefox ESR < 115.31, and Firefox ESR < 140.6.	8.8	More Details
CVE-	AVTECH SECURITY Corporation DGM1104 FullImg-1015-1004-1006-1003 was discovered to contain an authenticated command injection		More

2025-57199	vulnerability in the NetFailDetectD binary. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	8.8	Details
CVE-2025-14136	A security flaw has been discovered in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This vulnerability affects the function RE2000v2Repeater_get_wired_clientlist_setClientsName of the file mod_form.so. The manipulation of the argument clientsname_0 results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-12744	A flaw was found in the ABRT daemon’s handling of user-supplied mount information.ABRT copies up to 12 characters from an untrusted input and places them directly into a shell command (docker inspect %s) without proper validation. An unprivileged local user can craft a payload that injects shell metacharacters, causing the root-running ABRT process to execute attacker-controlled commands and ultimately gain full root privileges.	8.8	More Details
CVE-2025-14107	A security flaw has been discovered in ZSPACE Q2C NAS up to 1.1.0210050. Affected by this vulnerability is the function zfilev2_api.SafeStatus of the file /v2/file/safe/status of the component HTTP POST Request Handler. The manipulation of the argument safe_dir results in command injection. 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-2025-14108	A weakness has been identified in ZSPACE Q2C NAS up to 1.1.0210050. Affected by this issue is the function zfilev2_api.OpenSafe of the file /v2/file/safe/open of the component HTTP POST Request Handler. This manipulation of the argument safe_dir causes 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.	8.8	More Details
CVE-2025-12966	The All-in-One Video Gallery plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the resolve_import_directory() function in versions 4.5.4 to 4.5.7. This makes it possible for authenticated attackers, with Author-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-2025-66287	A flaw was found in WebKitGTK. Processing malicious web content can cause an unexpected process crash due to improper memory handling.	8.8	More Details
CVE-2025-14106	A vulnerability was identified in ZSPACE Q2C NAS up to 1.1.0210050. Affected is the function zfilev2_api.CloseSafe of the file /v2/file/safe/close of the component HTTP POST Request Handler. The manipulation of the argument safe_dir leads to command injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-13065	The Starter Templates plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 4.4.41. This is due to insufficient file type validation detecting WXR files, allowing double extension files to bypass sanitization while being accepted as a valid WXR file. This makes it possible for authenticated attackers, with author-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-2025-14126	A vulnerability has been found in TOZED ZLT M30S and ZLT M30S PRO 1.47/3.09.06. Affected is an unknown function of the component Web Interface. Such manipulation leads to hard-coded credentials. The attack needs to be initiated within the local network. 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.	8.8	More Details
CVE-2025-14134	A vulnerability was determined in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected by this issue is the function RE2000v2Repeater_get_wireless_clientlist_setClientsName of the file mod_form.so. Executing manipulation of the argument clientsname_0 can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-14135	A vulnerability was identified in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function AP_get_wired_clientlist_setClientsName of the file mod_form.so. The manipulation of the argument clientsname_0 leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-14133	A vulnerability was found in Linksys RE6500, RE6250, RE6300, RE6350, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected by this vulnerability is the function AP_get_wireless_clientlist_setClientsName of the file mod_form.so. Performing manipulation of the argument clientsname_0 results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-64678	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-57198	AVTECH SECURITY Corporation DGM1104 FullImg-1015-1004-1006-1003 was discovered to contain an authenticated command injection vulnerability in the Machine.cgi endpoint. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	8.8	More Details
CVE-2025-14141	A flaw has been found in UTT 进取 520W 1.7.7-180627. The impacted element is the function strcpy of the file /goform/formArpBindConfig. Executing manipulation of the argument pools can lead to buffer overflow. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-65959	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.37, a Stored XSS vulnerability was discovered in Open-WebUI's Notes PDF download functionality. An attacker can import a Markdown file containing malicious SVG tags into Notes, allowing them to execute arbitrary JavaScript code and steal session tokens when a victim downloads the note as PDF. This vulnerability can be exploited by any authenticated user, and unauthenticated external attackers can steal session tokens from users (both admin and regular users) by sharing specially crafted markdown files. This vulnerability is fixed in 0.6.37.	8.7	More Details
CVE-2025-12956	A reflected Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-26487	Server-Side Request Forgery (SSRF) vulnerability in Infinera MTC-9 version allows remote unauthenticated users to gain access to other network resources using HTTPS requests through the appliance used as a bridge.	8.6	More Details

CVE-2025-65958	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.37, a Server-Side Request Forgery (SSRF) vulnerability in Open WebUI allows any authenticated user to force the server to make HTTP requests to arbitrary URLs. This can be exploited to access cloud metadata endpoints (AWS/GCP/Azure), scan internal networks, access internal services behind firewalls, and exfiltrate sensitive information. No special permissions beyond basic authentication are required. This vulnerability is fixed in 0.6.37.	8.5	More Details
CVE-2025-64671	Improper neutralization of special elements used in a command ('command injection') in Copilot allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2025-65883	A vulnerability has been identified in Genexis Platinum P4410 router (Firmware P4410-V2–1.41) that allows a local network attacker to achieve Remote Code Execution (RCE) with root privileges. The issue occurs due to improper session invalidation after administrator logout. When an administrator logs out, the session token remains valid. An attacker on the local network can reuse this stale token to send crafted requests via the router’s diagnostic endpoint, resulting in command execution as root.	8.4	More Details
CVE-2025-50360	A heap buffer overflow in compiler.c and compiler.h in Pepper language 0.1.1commit 961a5d9988c5986d563310275adad3fd181b2bb7. Malicious execution of a pepper source file(.pr) could lead to arbitrary code execution or Denial of Service.	8.4	More Details
CVE-2025-62554	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2025-66627	Wasmi is a WebAssembly interpreter focused on constrained and embedded systems. In versions 0.41.0, 0.41.1, 0.42.0 through 0.47.1, 0.50.0 through 0.51.2 and 1.0.0, Wasmi's linear memory implementation leads to a Use After Free vulnerability, triggered by a WebAssembly module under certain memory growth conditions. This issue potentially leads to memory corruption, information disclosure, or code execution. This issue is fixed in versions 0.41.2, 0.47.1, 0.51.3 and 1.0.1. To workaround this issue, consider limiting the maximum linear memory sizes where feasible.	8.4	More Details
CVE-2025-62557	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2025-66324	Input verification vulnerability in the compression and decompression module. Impact: Successful exploitation of this vulnerability may affect app data integrity.	8.4	More Details
CVE-2025-66328	Multi-thread race condition vulnerability in the network management module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2025-65036	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Prior to 1.27.1, the macro executes Velocity from the details pages without checking for permissions, which can lead to remote code execution. This vulnerability is fixed in 1.27.1.	8.3	More Details
CVE-2025-40937	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected application do not properly validate input parameters in its REST API, resulting in improper handling of unexpected arguments. This could allow an authenticated attacker to execute arbitrary code with limited privileges.	8.3	More Details
CVE-2025-58098	Apache HTTP Server 2.4.65 and earlier with Server Side Includes (SSI) enabled and mod_cgid (but not mod_cgi) passes the shell-escaped query string to #exec cmd="..." directives. This issue affects Apache HTTP Server before 2.4.66. Users are recommended to upgrade to version 2.4.66, which fixes the issue.	8.3	More Details
CVE-2025-64057	Directory traversal vulnerability in Fanvil x210 V2 2.12.20 allows unauthenticated attackers on the local network to store files in arbitrary locations and potentially modify the system configuration or other unspecified impacts.	8.3	More Details
CVE-2025-63057	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Roxnor Wp Ultimate Review wp-ultimate-review allows DOM-Based XSS.This issue affects Wp Ultimate Review: from n/a through <= 2.3.6.	8.2	More Details
CVE-2025-42878	SAP Web Dispatcher and ICM may expose internal testing interfaces that are not intended for production. If enabled, unauthenticated attackers could exploit them to access diagnostics, send crafted requests, or disrupt services. This vulnerability has a high impact on confidentiality, availability and low impact on integrity and of the application.	8.2	More Details
CVE-2025-64447	A reliance on cookies without validation and integrity checking vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.5, FortiWeb 7.4.0 through 7.4.10, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow an unauthenticated attacker to execute arbitrary operations on the system via crafted HTTP or HTTPS request via forged cookies, requiring prior knowledge of the FortiWeb serial number.	8.1	More Details
CVE-2025-40801	A vulnerability has been identified in COMOS V10.6 (All versions), COMOS V10.6 (All versions), JT Bi-Directional Translator for STEP (All versions), NX V2412 (All versions < V2412.8900 with Cloud Entitlement (bundled as NX X)), NX V2506 (All versions < V2506.6000 with Cloud Entitlement (bundled as NX X)), Simcenter 3D (All versions < V2506.6000 with Cloud Entitlement (bundled as Simcenter X Mechanical)), Simcenter Femap (All versions < V2506.0002 with Cloud Entitlement (bundled as Simcenter X Mechanical)), Simcenter Studio (All versions), Simcenter System Architect (All versions), Tecnomatix Plant Simulation (All versions < V2504.0007). The SALT SDK is missing server certificate validation while establishing TLS connections to the authorization server. This could allow an attacker to perform a man-in-the-middle attack.	8.1	More Details
CVE-2025-13614	The Cool Tag Cloud plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cool_tag_cloud' shortcode in all versions up to, and including, 2.29 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.	8.1	More Details
CVE-2025-66626	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Versions 3.6.13 and below and versions 3.7.0 through 3.7.4, contain unsafe untar code that handles symbolic links in archives. Concretely, the computation of a link's target and the subsequent check are flawed. An attacker can overwrite the file /var/run/argo/argoexec with a script of their choice, which would be executed at the pod's start. The patch deployed against CVE-2025-62156 is ineffective against malicious archives containing symbolic links. This issue is fixed in versions 3.6.14 and 3.7.5.	8.1	More Details

CVE-2025-14333	Memory safety bugs present in Firefox ESR 140.5, Thunderbird ESR 140.5, Firefox 145 and Thunderbird 145. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 146 and Firefox ESR < 140.6.	8.1	More Details
CVE-2025-12851	The My auctions allegro plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.6.32 via the 'controller' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary 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 images and other “safe” file types can be uploaded and included.	8.1	More Details
CVE-2025-40938	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected device stores sensitive information in the firmware. This could allow an attacker to access and misuse this information, potentially impacting the device’s confidentiality, integrity, and availability.	8.1	More Details
CVE-2025-65879	Warehouse Management System 1.2 contains an authenticated arbitrary file deletion vulnerability. The /goods/deleteGoods endpoint accepts a user-controlled goodsimg parameter, which is directly concatenated with the server's UPLOAD_PATH and passed to File.delete() without validation. A remote authenticated attacker can delete arbitrary files on the server by supplying directory traversal payloads.	8.1	More Details
CVE-2025-12995	Medtronic CareLink Network allows an unauthenticated remote attacker to perform a brute force attack on an API endpoint that could be used to determine a valid password under certain circumstances. This issue affects CareLink Network: before December 4, 2025.	8.1	More Details
CVE-2025-20386	In Splunk Enterprise for Windows versions below 10.0.2, 9.4.6, 9.3.8, and 9.2.10, a new installation of or an upgrade to an affected version can result in incorrect permissions assignment in the Splunk Enterprise for Windows Installation directory. This lets non-administrator users on the machine access the directory and all its contents.	8.0	More Details
CVE-2025-67495	ZITADEL is an open-source identity infrastructure tool. Versions 4.0.0-rc.1 through 4.7.0 are vulnerable to DOM-Based XSS through the Zitadel V2 logout endpoint. The /logout endpoint insecurely routes to a value that is supplied in the post_logout_redirect GET parameter. As a result, unauthenticated remote attacker can execute malicious JS code on Zitadel users’ browsers. To carry out an attack, multiple user sessions need to be active in the same browser, however, account takeover is mitigated when using Multi-Factor Authentication (MFA) or Passwordless authentication. This issue is fixed in version 4.7.1.	8.0	More Details
CVE-2025-20387	In Splunk Universal Forwarder for Windows versions below 10.0.2, 9.4.6, 9.3.8, and 9.2.10, a new installation of or an upgrade to an affected version can result in incorrect permissions assignment in the Universal Forwarder for Windows Installation directory. This lets non-administrator users on the machine access the directory and all its contents.	8.0	More Details
CVE-2025-14322	Sandbox escape due to incorrect boundary conditions in the Graphics: CanvasWebGL component. This vulnerability affects Firefox < 146, Firefox ESR < 115.31, and Firefox ESR < 140.6.	8.0	More Details
CVE-2025-65806	The E-POINT CMS eagle.gsam-1169.1 file upload feature improperly handles nested archive files. An attacker can upload a nested ZIP (a ZIP containing another ZIP) where the inner archive contains an executable file (e.g. webshell.php). When the application extracts the uploaded archives, the executable may be extracted into a web-accessible directory. This can lead to remote code execution (RCE), data disclosure, account compromise, or further system compromise depending on the web server/process privileges. The issue arises from insufficient validation of archive contents and inadequate restrictions on extraction targets.	8.0	More Details
CVE-2025-54065	GZDoom is a feature centric port for all Doom engine games. GZDoom is an open source Doom engine. In versions 4.14.2 and earlier, ZScript actor state handling allows scripts to read arbitrary addresses, write constants into the JIT-compiled code section, and redirect control flow through crafted FState and VMFunction structures. A script can copy FState structures into a writable buffer, modify function pointers and state transitions, and cause execution of attacker-controlled bytecode, leading to arbitrary code execution.	7.9	More Details
CVE-2025-42874	SAP NetWeaver remote service for Xcelsius allows an attacker with network access and high privileges to execute arbitrary code on the affected system due to insufficient input validation and improper handling of remote method calls. Exploitation does not require user interaction and could lead to service disruption or unauthorized system control. This has high impact on integrity and availability, with no impact on confidentiality.	7.9	More Details
CVE-2025-48580	In connectInternal of MediaBrowser.java, there is a possible way to access while in use permission while the app is in background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48583	In multiple functions of BaseBundle.java, there is a possible way to execute arbitrary code due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54100	Improper neutralization of special elements used in a command ('command injection') in Windows PowerShell allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-54305	An issue was discovered in the Thermo Fisher Torrent Suite Django application 5.18.1. One of the middlewares included in this application, LocalhostAuthMiddleware, authenticates users as ionadmin if the REMOTE_ADDR property in request.META is set to 127.0.0.1, to 127.0.1.1, or to ::1. Any user with local access to the server may bypass authentication.	7.8	More Details
CVE-2025-48596	In appendFrom of Parcel.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48575	In multiple functions of CertInstaller.java, there is a possible way to install certificates due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48573	In sendCommand of MediaSessionRecord.java, there is a possible way to launch the foreground service while the app is in the background due to FGS while-in-use abuse. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48586	In onActivityResult of EditFdnContactScreen.java, there is a possible way to leak contacts from the work profile due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE-2025-48588	In startAlwaysOnVpn of Vpn.java, there is a possible way to disable always-on VPN due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48589	In multiple functions of HeaderPrivacyIconsController.kt, there is a possible way to grand permissions across user due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48632	In setDisplayName of AssociationRequest.java, there is a possible way to cause CDM associations to persist after the user has disassociated them due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48597	In multiple locations, there is a possible way to trick a user into accepting a permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48629	In findAvailRecognizer of VoiceInteractionManagerService.java, there is a possible way to become the default speech recognizer app due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-54160	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in BeeDrive in Synology BeeDrive for desktop before 1.4.2-13960 allows local users to execute arbitrary code via unspecified vectors.	7.8	More Details
CVE-2025-54158	Missing authentication for critical function vulnerability in BeeDrive in Synology BeeDrive for desktop before 1.4.2-13960 allows local users to execute arbitrary code via unspecified vectors.	7.8	More Details
CVE-2025-55233	Out-of-bounds read in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-13662	Improper verification of cryptographic signatures in the patch management component of Ivanti Endpoint Manager prior to version 2024 SU4 SR1 allows a remote unauthenticated attacker to execute arbitrary code. User Interaction is required.	7.8	More Details
CVE-2025-48606	In preparePackage of InstallPackageHelper.java, there is a possible way for an app to appear hidden upon installation without a mechanism to uninstall it due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48638	In __pkvm_load_tracing of trace.c, there is a possible out-of-bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48637	In multiple functions of mem_protect.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48628	In validateIconUserBoundary of PrintManagerService.java, there is a possible cross-user image leak due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48599	In multiple functions of WifiScanModeActivity.java, there is a possible way to bypass a device config restriction due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48627	In startNextMatchingActivity of ActivityTaskManagerService.java, there is a possible way to launch an activity from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48624	In multiple functions of arm-smmu-v3.c, there is a possible out-of-bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-66533	Improper Control of Generation of Code ('Code Injection') vulnerability in StellarWP GiveWP give allows Code Injection.This issue affects GiveWP: from n/a through <= 4.13.1.	7.8	More Details
CVE-2025-48623	In init_pkvm_hyp_vcpu of pkvm.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48620	In onSomePackagesChanged of VoiceInteractionManagerService.java, there is a possible way for a third party application's component name to persist even after uninstalling due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48615	In getComponentName of MediaButtonReceiverHolder.java, there is a possible desync in persistence due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48612	In multiple locations, there is a possible way for an application on a work profile to set the main user's default NFC payment setting due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-48572	In multiple locations, there is a possible way to launch activities from the background due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-			

2025-62466	Null pointer dereference in Windows Client-Side Caching (CSC) Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59516	Missing authentication for critical function in Windows Storage VSP Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-66411	Coder allows organizations to provision remote development environments via Terraform. Prior to 2.26.5, 2.27.7, and 2.28.4, Workspace Agent manifests containing sensitive values were logged in plaintext unsanitized. An attacker with limited local access to the Coder Workspace (VM, K8s Pod etc.) or a third-party system (SIEM, logging stack) could access those logs. This vulnerability is fixed in 2.26.5, 2.27.7, and 2.28.4.	7.8	More Details
CVE-2025-62553	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62556	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62558	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62559	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62560	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-59517	Improper access control in Windows Storage VSP Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62562	Use after free in Microsoft Office Outlook allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62563	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62564	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-66431	WebPros Plesk before 18.0.73.5 and 18.0.74 before 18.0.74.2 on Linux allows remote authenticated users to execute arbitrary code as root via domain creation. The attacker needs "Create and manage sites" with "Domains management" and "Subdomains management."	7.8	More Details
CVE-2025-62571	Improper input validation in Windows Installer allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62572	Out-of-bounds read in Application Information Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-64661	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Shell allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-64673	Improper access control in Storvsp.sys Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-53841	The GC-AGENTS-SERVICE running as part of Akamai´s Guardicore Platform Agent for Windows versions prior to v49.20.1, v50.15.0, v51.12.0, v52.2.0 is affected by a local privilege escalation vulnerability. The service will attempt to read an OpenSSL configuration file from a non-existent location that standard Windows users have default write access to. This allows an unprivileged local user to create a crafted "openssl.cnf" file in that location and, by specifying the path to a custom DLL file in a custom OpenSSL engine definition, execute arbitrary commands with the privileges of the Guardicore Agent process. Since Guardicore Agent runs with SYSTEM privileges, this permits an unprivileged user to fully elevate privileges to SYSTEM level in this manner.	7.8	More Details
CVE-2025-64679	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-64680	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-64783	DNG SDK versions 1.7.0 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-	Acrobat Reader versions 24.001.30264, 20.005.30793, 25.001.20982, 24.001.30273, 20.005.30803 and earlier are affected by an		

2025-64785	Untrusted Search Path vulnerability that might allow attackers to execute arbitrary code in the context of the current user. If the application uses a search path to locate critical resources such as programs, an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue does not require user interaction.	7.8	More Details
CVE-2025-64899	Acrobat Reader versions 24.001.30264, 20.005.30793, 25.001.20982, 24.001.30273, 20.005.30803 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-67488	SiYuan is self-hosted, open source personal knowledge management software. Versions 0.0.0-20251202123337-6ef83b42c7ce and below contain function importZipMd which is vulnerable to ZipSlips, allowing an authenticated user to overwrite files on the system. An authenticated user with access to the import functionality in notes is able to overwrite any file on the system, and can escalate to full code execution under some circumstances. A fix is planned for version 3.5.0.	7.8	More Details
CVE-2025-62552	Relative path traversal in Microsoft Office Access allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62561	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62474	Improper access control in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48565	In multiple locations, there is a possible way to bypass the cross profile intent filter due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-62461	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62462	Buffer over-read in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48525	In disassociate of DisassociationProcessor.java, there is a possible way for an app to continue reading notifications when not associated to a companion device due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-62457	Out-of-bounds read in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62464	Buffer over-read in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48536	In grantAllowlistedPackagePermissions of SettingsSliceProvider.java, there is a possible way for a third party app to modify secure settings due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-32329	In multiple functions of Session.java, there is a possible way to view images belonging to a different user of the device due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-62455	Improper input validation in Windows Message Queuing allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62454	Heap-based buffer overflow in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62458	Heap-based buffer overflow in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48555	In multiple functions of NotificationStation.java, there is a possible cross-profile information disclosure due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-62221	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-48566	In multiple locations, there is a possible bypass of user profile boundary with a forwarded intent due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-62467	Integer overflow or wraparound in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-	In multiple functions of Session.java, there is a possible way to view images belonging to a different user of the device due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed	7.8	More

32328	for exploitation.		Details
CVE-2025-62470	Heap-based buffer overflow in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-22420	In multiple locations, there is a possible way to leak audio files across user profiles due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2025-62472	Use of uninitialized resource in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-7044	An Improper Input Validation vulnerability exists in the user websocket handler of MAAS. An authenticated, unprivileged attacker can intercept a user.update websocket request and inject the is_superuser property set to true. The server improperly validates this input, allowing the attacker to self-promote to an administrator role. This results in full administrative control over the MAAS deployment.	7.7	More Details
CVE-2025-65843	Aquarius Desktop 3.0.069 for macOS contains an insecure file handling vulnerability in its support data archive generation feature. The application follows symbolic links placed inside the ~/Library/Logs/Aquarius directory and treats them as regular files. When building the support ZIP, Aquarius recursively enumerates logs using a JUCE directory iterator configured to follow symlinks, and later writes file data without validating whether the target is a symbolic link. A local attacker can exploit this behavior by planting symlinks to arbitrary filesystem locations, resulting in unauthorized disclosure or modification of arbitrary files. When chained with the associated HelperTool privilege escalation issue, root-owned files may also be exposed.	7.7	More Details
CVE-2024-9183	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.4 prior to 18.4.5, 18.5 prior to 18.5.3, and 18.6 prior to 18.6.1 that could have allowed an authenticated user to obtain credentials from higher-privileged users and perform actions in their context under specific conditions.	7.7	More Details
CVE-2025-63062	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AndonDesign UDesign Core u-design-core allows PHP Local File Inclusion.This issue affects UDesign Core: from n/a through <= 4.14.0.	7.6	More Details
CVE-2025-65027	RomM (ROM Manager) allows users to scan, enrich, browse and play their game collections with a clean and responsive interface. RomM contains multiple unrestricted file upload vulnerabilities that allow authenticated users to upload malicious SVG or HTML files. When these files are accessed the browser executes embedded JavaScript, leading to stored Cross-Site Scripting (XSS) which when combined with a CSRF misconfiguration they lead to achieve full administrative account takeover, creating a rogue admin account, escalating the attacker account role to admin, and much more. This vulnerability is fixed in 4.4.1 and 4.4.1-beta.2.	7.6	More Details
CVE-2025-66624	BACnet Protocol Stack library provides a BACnet application layer, network layer and media access (MAC) layer communications services. Prior to 1.5.0.rc2, The npdu_is_expected_reply function in src/bacnet/npdu.c indexes request_pdu[offset+2/3/5] and reply_pdu[offset+1/2/4] without verifying that those APDU bytes exist. bacnet_npdu_decode() can return offset == 2 for a 2-byte NPDU, so tiny PDUs pass the version check and then get read out of bounds. On ASan/MPU/strict builds this is an immediate crash (DoS). On unprotected builds it is undefined behavior and can mis-route replies; RCE is unlikely because only reads occur, but DoS is reliable.	7.5	More Details
CVE-2025-12097	There is a relative path traversal vulnerability in the NI System Web Server that may result in information disclosure. Successful exploitation requires an attacker to send a specially crafted request to the NI System Web Server, allowing the attacker to read arbitrary files. This vulnerability existed in the NI System Web Server 2012 and prior versions. It was fixed in 2013.	7.5	More Details
CVE-2025-65637	A denial-of-service vulnerability exists in github.com/sirupsen/logrus when using Entry.Writer() to log a single-line payload larger than 64KB without newline characters. Due to limitations in the internal bufio.Scanner, the read fails with "token too long" and the writer pipe is closed, leaving Writer() unusable and causing application unavailability (DoS). This affects versions < 1.8.3, 1.9.0, and 1.9.2. The issue is fixed in 1.8.3, 1.9.1, and 1.9.3+, where the input is chunked and the writer continues to function even if an error is logged.	7.5	More Details
CVE-2025-40820	Affected products do not properly enforce TCP sequence number validation in specific scenarios but accept values within a broad range. This could allow an unauthenticated remote attacker e.g. to interfere with connection setup, potentially leading to a denial of service. The attack succeeds only if an attacker can inject IP packets with spoofed addresses at precisely timed moments, and it affects only TCP-based services.	7.5	More Details
CVE-2025-65878	The warehouse management system version 1.2 contains an arbitrary file read vulnerability. The endpoint `/file/showImageByPath` does not sanitize user-controlled path parameters. An attacker could exploit directory traversal to read arbitrary files on the server's file system. This could lead to the leakage of sensitive system information.	7.5	More Details
CVE-2025-13654	A stack buffer overflow vulnerability exists in the buffer_get function of duc, a disk management tool, where a condition can evaluate to true due to underflow, allowing an out-of-bounds read.	7.5	More Details
CVE-2025-64053	A Buffer overflow vulnerability on Fanvil x210 2.12.20 devices allows attackers to cause a denial of service or potentially execute arbitrary commands via crafted POST request to the /cgi-bin/webconfig?page=upload&action=submit endpoint.	7.5	More Details
CVE-2025-12850	The My auctions allegro plugin for WordPress is vulnerable to SQL Injection via the ‘auction_id’ parameter in all versions up to, and including, 3.6.32 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-14309	NULL Pointer Dereference vulnerability in ravynsoft ravynos.This issue affects ravynos: through 0.5.2.	7.5	More Details
CVE-2025-59775	Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server on Windows with AllowEncodedSlashes On and MergeSlashes Off allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.66, which fixes the issue.	7.5	More Details
CVE-2024-56836	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). During the Dynamic DNS configuration of the affected product it is possible to inject additional configuration parameters. Under certain circumstances, an attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.	7.5	More Details

CVE-2025-53704	The password reset mechanism for the Pivot client application is weak, and it may allow an attacker to take over the account.	7.5	More Details
CVE-2025-66506	Fulcio is a free-to-use certificate authority for issuing code signing certificates for an OpenID Connect (OIDC) identity. Prior to 1.8.3, function identity.extractIssuerURL splits (via a call to strings.Split) its argument (which is untrusted data) on periods. As a result, in the face of a malicious request with an (invalid) OIDC identity token in the payload containing many period characters, a call to extractIssuerURL incurs allocations to the tune of O(n) bytes (where n stands for the length of the function's argument), with a constant factor of about 16. This vulnerability is fixed in 1.8.3.	7.5	More Details
CVE-2025-55753	An integer overflow in the case of failed ACME certificate renewal leads, after a number of failures (~30 days in default configurations), to the backoff timer becoming 0. Attempts to renew the certificate then are repeated without delays until it succeeds. This issue affects Apache HTTP Server: from 2.4.30 before 2.4.66. Users are recommended to upgrade to version 2.4.66, which fixes the issue.	7.5	More Details
CVE-2025-13373	Advantech iView versions 5.7.05.7057 and prior do not properly sanitize SNMP v1 trap (Port 162) requests, which could allow an attacker to inject SQL commands.	7.5	More Details
CVE-2025-63363	A lack of Management Frame Protection in Waveshare RS232/485 TO WIFI ETH (B) Serial to Ethernet/Wi-Fi Gateway Firmware V3.1.1.0: HW 4.3.2.1: Webpage V7.04T.07.002880.0301 allows attackers to execute de-authentication attacks, allowing crafted deauthentication and disassociation frames to be broadcast without authentication or encryption.	7.5	More Details
CVE-2025-66564	Sigstore Timestamp Authority is a service for issuing RFC 3161 timestamps. Prior to 2.0.3, Function api.ParseJSONRequest currently splits (via a call to strings.Split) an optionally-provided OID (which is untrusted data) on periods. Similarly, function api.getContentType splits the Content-Type header (which is also untrusted data) on an application string. As a result, in the face of a malicious request with either an excessively long OID in the payload containing many period characters or a malformed Content-Type header, a call to api.ParseJSONRequest or api.getContentType incurs allocations of O(n) bytes (where n stands for the length of the function's argument). This vulnerability is fixed in 2.0.3.	7.5	More Details
CVE-2025-48592	In initDecoder of C2SoftDav1dDec.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2025-26488	Improper Input Validation vulnerability in Infinera MTC-9 allows remote unauthenticated users to crash the service and cause a reboot of the appliance, thus causing a DoS condition, via crafted XML payloads.This issue affects MTC-9: from R22.1.1.0275 before R23.0.	7.5	More Details
CVE-2025-48631	In onHeaderDecoded of LocalImageResolver.java, there is a possible persistent denial of service due to resource exhaustion. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2025-65795	Incorrect access control in the /api/v1/user endpoint of usememos memos v0.25.2 allows unauthorized attackers to create arbitrary accounts via a crafted request.	7.5	More Details
CVE-2025-65945	auth0/node-jws is a JSON Web Signature implementation for Node.js. In versions 3.2.2 and earlier and version 4.0.0, auth0/node-jws has an improper signature verification vulnerability when using the HS256 algorithm under specific conditions. Applications are affected when they use the jws.createVerify() function for HMAC algorithms and use user-provided data from the JSON Web Signature protected header or payload in HMAC secret lookup routines, which can allow attackers to bypass signature verification. This issue has been patched in versions 3.2.3 and 4.0.1.	7.5	More Details
CVE-2025-12819	Untrusted search path in auth_query connection handler in PgBouncer before 1.25.1 allows an unauthenticated attacker to execute arbitrary SQL during authentication via a malicious search_path parameter in the StartupMessage.	7.5	More Details
CVE-2024-45539	Out-of-bounds write vulnerability in cgi components in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 and 7.2.2-72806 and Synology Unified Controller (DSMUC) before 3.1.4-23079 allows remote attackers to conduct denial-of-service attacks via unspecified vectors.	7.5	More Details
CVE-2025-57210	Incorrect access control in the component ApiPayController.java of platform v1.0.0 allows attackers to access sensitive information via unspecified vectors.	7.5	More Details
CVE-2025-57212	Incorrect access control in the component ApiOrderService.java of platform v1.0.0 allows attackers to access sensitive information via a crafted request.	7.5	More Details
CVE-2025-64658	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Shell allows an authorized attacker to elevate privileges locally.	7.5	More Details
CVE-2024-3884	A flaw was found in Undertow that can cause remote denial of service attacks. When the server uses the FormEncodedDataDefinition.doParse(StreamSourceChannel) method to parse large form data encoding with application/x-www-form-urlencoded, the method will cause an OutOfMemory issue. This flaw allows unauthorized users to cause a remote denial of service (DoS) attack.	7.5	More Details
CVE-2025-57213	Incorrect access control in the component orderService.queryObject of platform v1.0.0 allows attackers to access sensitive information via a crafted request.	7.5	More Details
CVE-2025-42877	SAP Web Dispatcher, Internet Communication Manager (ICM), and SAP Content Server allow an unauthenticated user to exploit logical errors that lead to a memory corruption vulnerability. This results in high impact on the availability with no impact on confidentiality or integrity of the application.	7.5	More Details
CVE-2025-64666	Improper input validation in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details

CVE-2024-32643	Masa CMS is an open source Enterprise Content Management platform. Prior to 7.2.8, 7.3.13, and 7.4.6, if the URL to the page is modified to include a /tag/ declaration, the CMS will render the page regardless of group restrictions. This vulnerability is fixed in 7.2.8, 7.3.13, and 7.4.6.	7.5	More Details
CVE-2025-63364	Waveshare RS232/485 TO WIFI ETH (B) Serial to Ethernet/Wi-Fi Gateway Firmware V3.1.1.0: HW 4.3.2.1: Webpage V7.04T.07.002880.0301 was discovered to transmit Administrator credentials in plaintext.	7.5	More Details
CVE-2025-65320	Abacre Restaurant Point of Sale (POS) up to 15.0.0.1656 are vulnerable to Cleartext Storage of Sensitive Information in Memory. The application leaves valid device-bound license keys in process memory during an activation attempt.	7.5	More Details
CVE-2025-56427	Directory Traversal vulnerability in ComposioHQ v.0.7.20 allows a remote attacker to obtain sensitive information via the _download_file_or_dir function.	7.5	More Details
CVE-2025-59030	An attacker can trigger the removal of cached records by sending a NOTIFY query over TCP.	7.5	More Details
CVE-2025-33211	NVIDIA Triton Server for Linux contains a vulnerability where an attacker may cause an improper validation of specified quantity in input. A successful exploit of this vulnerability may lead to denial of service.	7.5	More Details
CVE-2025-66507	1Panel is an open-source, web-based control panel for Linux server management. Versions 2.0.13 and below allow an unauthenticated attacker to disable CAPTCHA verification by abusing a client-controlled parameter. Because the server previously trusted this value without proper validation, CAPTCHA protections can be bypassed, enabling automated login attempts and significantly increasing the risk of account takeover (ATO). This issue is fixed in version 2.0.14.	7.5	More Details
CVE-2025-63076	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Dream-Theme The7 Elements dt-the7-core allows PHP Local File Inclusion.This issue affects The7 Elements: from n/a through <= 2.7.11.	7.5	More Details
CVE-2025-63074	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Dream-Theme The7 dt-the7 allows PHP Local File Inclusion.This issue affects The7: from n/a through <= 12.8.0.2.	7.5	More Details
CVE-2025-33201	NVIDIA Triton Inference Server contains a vulnerability where an attacker may cause an improper check for unusual or exceptional conditions issue by sending extra large payloads. A successful exploit of this vulnerability may lead to denial of service.	7.5	More Details
CVE-2025-54326	An issue was discovered in Camera in Samsung Mobile Processor Exynos 1280 and 2200. Unnecessary registration of a hardware IP address in the Camera device driver can lead to a NULL pointer dereference, resulting in a denial of service.	7.5	More Details
CVE-2025-66645	NiceGUI is a Python-based UI framework. Versions 3.3.1 and below are vulnerable to directory traversal through the App.add_media_files() function, which allows a remote attacker to read arbitrary files on the server filesystem. This issue is fixed in version 3.4.0.	7.5	More Details
CVE-2025-13646	The Modula Image Gallery plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'ajax_unzip_file' function in versions 2.13.1 to 2.13.2. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files with race condition on the affected site's server which may make remote code execution possible.	7.5	More Details
CVE-2025-54159	Missing authorization vulnerability in BeeDrive in Synology BeeDrive for desktop before 1.4.2-13960 allows remote attackers to delete arbitrary files via unspecified vectors.	7.5	More Details
CVE-2025-66623	Strimzi provides a way to run an Apache Kafka cluster on Kubernetes or OpenShift in various deployment configurations. From 0.47.0 and prior to 0.49.1, in some situations, Strimzi creates an incorrect Kubernetes Role which grants the Apache Kafka Connect and Apache Kafka MirrorMaker 2 operands the GET access to all Kubernetes Secrets that exist in the given Kubernetes namespace. The issue is fixed in Strimzi 0.49.1.	7.4	More Details
CVE-2025-40800	A vulnerability has been identified in COMOS V10.6 (All versions), COMOS V10.6 (All versions), NX V2412 (All versions < V2412.8700), NX V2506 (All versions < V2506.6000), Simcenter 3D (All versions < V2506.6000), Simcenter Femap (All versions < V2506.0002), Solid Edge SE2025 (All versions < V225.0 Update 10), Solid Edge SE2026 (All versions < V226.0 Update 1). The IAM client in affected products is missing server certificate validation while establishing TLS connections to the authorization server. This could allow an attacker to perform a man-in-the-middle attack.	7.4	More Details
CVE-2025-13947	A flaw was found in WebKitGTK. This vulnerability allows remote, user-assisted information disclosure that can reveal any file the user is permitted to read via abusing the file drag-and-drop mechanism where WebKitGTK does not verify that drag operations originate from outside the browser.	7.4	More Details
CVE-2025-14251	A security vulnerability has been detected in code-projects Online Ordering System 1.0. This affects an unknown function of the file /admin/ of the component Admin Login. Such manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-14250	A weakness has been identified in code-projects Online Ordering System 1.0. The impacted element is an unknown function of the file /user_contact.php. This manipulation of the argument Name causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-14249	A security flaw has been discovered in code-projects Online Ordering System 1.0. The affected element is an unknown function of the file /user_school.php. The manipulation of the argument product_id results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-14257	A flaw has been found in itsourcecode Student Management System 1.0. Affected is an unknown function of the file /newrecord.php. Executing manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	7.3	More Details

CVE-2025-14248	A vulnerability was identified in code-projects Simple Shopping Cart 1.0. Impacted is an unknown function of the file /adminlogin.php. The manipulation of the argument admin_username leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14245	A vulnerability has been found in IdeaCMS up to 1.8. This affects the function whereRaw of the file app/common/logic/index/Coupon.php. Such manipulation of the argument params leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-48594	In onUidImportance of DisassociationProcessor.java, there is a possible way to retain companion application privileges after disassociation due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-14226	A vulnerability was identified in itsourcecode Student Management System 1.0. This vulnerability affects unknown code of the file /edit_user.php. The manipulation of the argument fname leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-48621	In DefaultTransitionHandler.java, there is a possible way to enable a tapjacking attack due to a insecure default. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-48639	In DefaultTransitionHandler.java, there is a possible way to unknowingly grant permissions to an app due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2025-14256	A vulnerability was detected in itsourcecode Student Management System 1.0. This impacts an unknown function of the file /newcurriculm.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-14215	A vulnerability was found in code-projects Currency Exchange System 1.0. This vulnerability affects unknown code of the file /edit.php. 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.	7.3	More Details
CVE-2025-62565	Use after free in Windows Shell allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2025-14223	A vulnerability has been found in code-projects Simple Leave Manager 1.0. Affected by this vulnerability is an unknown functionality of the file /request.php. Such manipulation of the argument staff_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-14337	A vulnerability was determined in itsourcecode Student Management System 1.0. This affects an unknown part of the file /new_grade.php. This manipulation of the argument grade causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-14336	A vulnerability was found in itsourcecode Student Management System 1.0. Affected by this issue is some unknown functionality of the file /promote.php. The manipulation of the argument sy 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-2025-14335	A vulnerability has been found in itsourcecode Student Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /new_school_year.php. The manipulation of the argument sy 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-2025-14334	A flaw has been found in itsourcecode Student Management System 1.0. Affected is an unknown function of the file /new_adviser.php. Executing manipulation of the argument Name 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-2025-14189	A vulnerability was detected in Chanjet CRM up to 20251121. Affected is an unknown function of the file /tools/jxf_dump_table_demo.php. The manipulation of the argument gblOrgID results in sql injection. 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.	7.3	More Details
CVE-2025-14190	A flaw has been found in Chanjet TPlus up to 20251121. Affected by this vulnerability is an unknown functionality of the file /tplus/ajaxpro/Ufida.T.SM.UIP.MultiCompanySettingController,Ufida.T.SM.UIP.ashx?method=Load. This manipulation of the argument currentAccId causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-14192	A vulnerability was found in RashminDungrani online-banking up to 2337ad552ea9d385b4e07b90e6f32d011b7c68a2. This affects an unknown part of the file /site/dist/auth_login.php. Performing manipulation of the argument Username results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-14207	A vulnerability was identified in tushar-2223 Hotel-Management-System up to bb1f3b3666124b888f1e4bcf51b6fba9fbb01d15. The impacted element is an unknown function of the file /admin/invoiceprint.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	7.3	More Details
CVE-2025-14209	A weakness has been identified in Campcodes School File Management System 1.0. This impacts an unknown function of the file /update_query.php. This manipulation of the argument stud_id causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-14210	A security vulnerability has been detected in projectworlds Advanced Library Management System 1.0. Affected is an unknown function of the file /delete_member.php. Such manipulation of the argument user_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-2025-14211	A vulnerability was detected in projectworlds Advanced Library Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /delete_book.php. Performing manipulation of the argument book_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-2025-14212	A flaw has been found in projectworlds Advanced Library Management System 1.0. Affected by this issue is some unknown functionality of the file /member_search.php. Executing manipulation of the argument roll_number 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-2025-66561	SysReptor is a fully customizable pentest reporting platform. Prior to 2025.102, there is a Stored Cross-Site Scripting (XSS) vulnerability allows authenticated users to execute malicious JavaScript in the context of other logged-in users by uploading malicious JavaScript files in the web UI. This vulnerability is fixed in 2025.102.	7.3	More Details
CVE-2025-14216	A vulnerability was determined in code-projects Currency Exchange System 1.0. This issue affects some unknown processing of the file /viewserial.php. 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.	7.3	More Details
CVE-2025-14091	A weakness has been identified in TrippWasTaken PHP-Guitar-Shop up to 6ce0868889617c1975982aae6df8e49555d0d555. This vulnerability affects unknown code of the file /product.php of the component Product Details Page. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-14217	A vulnerability was identified in code-projects Currency Exchange System 1.0. Impacted is an unknown function of the file /edittrns.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14218	A security flaw has been discovered in code-projects Currency Exchange System 1.0. The affected element is an unknown function of the file /editotheraccount.php. Performing manipulation of the argument ID 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-2025-14258	A vulnerability has been found in itsourcecode Student Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /newsubject.php. The manipulation of the argument sub leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-46637	Dell Encryption, versions prior to 11.12.1, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A local malicious user could potentially exploit this vulnerability, leading to Elevation of privileges.	7.3	More Details
CVE-2025-14332	Memory safety bugs present in Firefox 145 and Thunderbird 145. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 146.	7.3	More Details
CVE-2025-14285	A vulnerability was found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file edit_personnel.php. The manipulation of the argument per_id 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-2025-55948	This vulnerability fundamentally arises from yzcheng90 X-SpringBoot 6.0's implementation of role-based access control (RBAC) through dual dependency on frontend menu systems and backend permission tables, without enforcing atomic synchronization between these components. The critical flaw manifests when frontend menu updates (such as privilege revocation) fail to propagate to the backend permission table in real-time, creating a dangerous desynchronization. While users lose access to restricted functions through the web interface (as UI elements properly disappear), the stale permission records still validate unauthorized API requests when accessed directly through tools like Postman. Attackers exploiting this inconsistency can perform privileged operations including but not limited to: creating high-permission user accounts, accessing sensitive data beyond their clearance level, and executing admin-level commands.	7.3	More Details
CVE-2025-14325	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 146 and Firefox ESR < 140.6.	7.3	More Details
CVE-2024-56840	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). Under certain conditions, IPsec may allow code injection in the affected device. An attacker could leverage this scenario to execute arbitrary code as root user.	7.2	More Details
CVE-2025-64156	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiVoice 7.2.0 through 7.2.1, FortiVoice 7.0.0 through 7.0.7, FortiVoice 6.4 all versions, FortiVoice 6.0 all versions may allow an authenticated privileged attacker to execute unauthorized code or commands via crafted requests	7.2	More Details
CVE-2025-64153	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiExtender 7.6.0 through 7.6.3, FortiExtender 7.4.0 through 7.4.7, FortiExtender 7.2 all versions, FortiExtender 7.0 all versions may allow an authenticated attacker to execute unauthorized code or commands via a specific HTTP request.	7.2	More Details
CVE-2025-13604	The Login Security, FireWall, Malware removal by CleanTalk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the page URL in all versions up to, and including, 2.168 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-12705	The Social Reviews & Recommendations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in the 'trim_text' function in all versions up to, and including, 2.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 2.5.	7.2	More Details
CVE-2025-54306	An issue was discovered in the Thermo Fisher Torrent Suite Django application 5.18.1. A remote code execution vulnerability exists in the network configuration functionality, stemming from insufficient input validation when processing network configuration parameters through administrative endpoints. The application allows administrators to modify the server's network configuration through the Django application. This configuration is processed by Bash scripts (TSsetnoproxy and TSsetproxy) that write user-controlled data directly to environment variables without proper sanitization. After updating environment variables, the scripts execute a source command on /etc/environment; if an attacker injects malicious data into environment variables, this command can enable arbitrary command execution. The vulnerability begins with the /admin/network endpoint, which passes user-supplied form data as arguments to subprocess.Popen calls. The user-supplied input is then used to update environment variables in TSsetnoproxy and TSsetproxy, and finally source $environment is executed.	7.2	More Details
CVE-2025-	A weakness has been identified in UGREEN DH2100+ up to 5.3.0.251125. This affects the function handler_file_backup_create of the file /v1/file/backup/create of the component nas_svr. Executing manipulation of the argument path can lead to buffer overflow. The attack can	7.2	More

14187	be executed 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.		Details
CVE-2025-53679	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiSandbox version 5.0.0 through 5.0.2 and before 4.4.7 GUI allows a remote privileged attacker to execute unauthorized code or commands via crafted HTTP or HTTPS requests.	7.2	More Details
CVE-2025-53949	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.0 through 4.4.7, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may allow an authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests.	7.2	More Details
CVE-2024-56839	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). Code injection can be achieved when the affected device is using VRF (Virtual Routing and Forwarding). An attacker could leverage this scenario to execute arbitrary code as root user.	7.2	More Details
CVE-2025-29846	A vulnerability in portenable cgi allows remote authenticated users to get the status of installed packages.	7.2	More Details
CVE-2024-56838	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). The SCEP client available in the affected device for secure certificate enrollment lacks validation of multiple fields. An attacker could leverage this scenario to execute arbitrary code as root user.	7.2	More Details
CVE-2024-56837	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). Due to the insufficient validation during the installation and load of certain configuration files of the affected device, an attacker could spawn a reverse shell and gain root access on the affected system.	7.2	More Details
CVE-2025-14188	A security vulnerability has been detected in UGREEN DH2100+ up to 5.3.0.251125. This impacts the function handler_file_backup_create of the file /v1/file/backup/create of the component nas_svr. The manipulation of the argument path leads to command injection. 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.	7.2	More Details
CVE-2025-11727	The Omnichannel for WooCommerce: Google, Amazon, eBay & Walmart Integration – Powered by Codisto plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the sync() function in all versions up to, and including, 1.3.65 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-66238	DCIM dcTrack allows an attacker to misuse certain remote access features. An authenticated user with access to the appliance's virtual console could exploit these features to redirect network traffic, potentially accessing restricted services or data on the host machine.	7.2	More Details
CVE-2025-66644	Array Networks ArrayOS AG before 9.4.5.9 allows command injection, as exploited in the wild in August through December 2025.	7.2	More Details
CVE-2025-13645	The Modula Image Gallery plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'ajax_unzip_file' function in versions 2.13.1 to 2.13.2. This makes it possible for authenticated attackers, with Author-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	7.2	More Details
CVE-2025-65363	Authenticated append-style command-injection Ruijie APs (AP_RGOS 11.1.x) allows an authenticated web user to execute appended shell expressions as root, enabling file disclosure, device disruption, and potential network pivoting via the command parameter to the web_action.do endpoint.	7.2	More Details
CVE-2025-12510	The Widgets for Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 13.2.4 due to insufficient input sanitization and output escaping on Google Reviews data imported by the plugin. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute in the admin panel (and potentially on the frontend) whenever a user accesses imported reviews, granted they can add a malicious review to a Google Place that is connected to the vulnerable site.	7.2	More Details
CVE-2025-12499	The Rich Shortcodes for Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the contents of a Google Review in all versions up to, and including, 6.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: This vulnerability was partially patched in version 6.6.2.	7.2	More Details
CVE-2025-41751	An XSS vulnerability in pxc_portCntr.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-41746	An XSS vulnerability in pxc_portSecCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-14261	The Litmus platform uses JWT for authentication and authorization, but the secret being used for signing the JWT is only 6 bytes long at its core, which makes it extremely easy to crack.	7.1	More Details
CVE-2025-41749	An XSS vulnerability in port_util.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
	An XSS vulnerability in pxc_portCntr2.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a		

CVE-2025-41745	manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-41747	An XSS vulnerability in pxc_vlanIntfCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-66293	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. Prior to 1.6.52, an out-of-bounds read vulnerability in libpng's simplified API allows reading up to 1012 bytes beyond the png_sRGB_base[512] array when processing valid palette PNG images with partial transparency and gamma correction. The PNG files that trigger this vulnerability are valid per the PNG specification; the bug is in libpng's internal state management. Upgrade to libpng 1.6.52 or later.	7.1	More Details
CVE-2025-66327	Race condition vulnerability in the network module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.1	More Details
CVE-2025-64784	DNG SDK versions 1.7.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure or application denial of service. An attacker could leverage this vulnerability to disclose sensitive memory information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.1	More Details
CVE-2025-13661	Path traversal in Ivanti Endpoint Manager prior to version 2024 SU4 SR1 allows a remote authenticated attacker to write arbitrary files outside of the intended directory. User interaction is required.	7.1	More Details
CVE-2025-62570	Improper access control in Windows Camera Frame Server Monitor allows an authorized attacker to disclose information locally.	7.1	More Details
CVE-2025-67541	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lester Chan WP-ShowHide wp-showhide allows Stored XSS.This issue affects WP-ShowHide: from n/a through <= 1.05.	7.1	More Details
CVE-2025-41695	An XSS vulnerability in dyn_conn.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-41750	An XSS vulnerability in pxc_PortCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-64893	DNG SDK versions 1.7.0 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure or application denial of service. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.1	More Details
CVE-2025-42876	Due to a Missing Authorization Check vulnerability in SAP S/4 HANA Private Cloud (Financials General Ledger), an authenticated attacker with authorization limited to a single company code could read sensitive data and post or modify documents across all company codes. Successful exploitation could result in a high impact to confidentiality and a low impact to integrity, while availability remains unaffected.	7.1	More Details
CVE-2025-41752	An XSS vulnerability in pxc_portSfp.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-41748	An XSS vulnerability in pxc_Dot1xCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.	7.1	More Details
CVE-2025-62569	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-62573	Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-46603	Dell CloudBoost Virtual Appliance, versions 19.13.0.0 and prior, contains an Improper Restriction of Excessive Authentication Attempts vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.0	More Details
CVE-2025-66214	Ladybug adds message-based debugging, unit, system, and regression testing to Java applications. Versions prior to 3.0-20251107.114628 contain the APIs /iaf/ladybug/api/report/{storage} and /iaf/ladybug/api/report/upload, which allow uploading gzip-compressed XML files with user-controllable content. The system deserializes these XML files, enabling attackers to achieve Remote Code Execution (RCE) by submitting carefully crafted XML payloads and thereby gain access to the target server. This issue is fixed in version 3.0-20251107.114628.	7.0	More Details
CVE-			

2025-62469	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-13492	A potential security vulnerability has been identified in HP Image Assistant for versions prior to 5.3.3. The vulnerability could potentially allow a local attacker to escalate privileges via a race condition when installing packages.	7.0	More Details
CVE-2025-62555	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-48625	In multiple locations of UsbDataAdvancedProtectionHook.java, there is a possible way to access USB data when the screen is off due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2025-48564	In multiple locations, there is a possible intent filter bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2025-54838	An Incorrect Authorization vulnerability [CWE-863] in FortiPortal 7.4.0 through 7.4.5 may allow an authenticated attacker to reboot a shared FortiGate device via crafted HTTP requests.	6.8	More Details
CVE-2025-48618	In processLaunchBrowser of CommandParamsFactory.java, there is a possible browser interaction from the lockscreen due to improper locking. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2025-41692	A high privileged remote attacker with admin privileges for the webUI can brute-force the "root" and "user" passwords of the underlying OS due to a weak password generation algorithm.	6.8	More Details
CVE-2025-41697	An attacker can use an undocumented UART port on the PCB as a side-channel to get root access e.g. with the credentials obtained from CVE-2025-41692.	6.8	More Details
CVE-2025-59808	An unverified password change vulnerability [CWE-620] vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.2, FortiSOAR PaaS 7.5.0 through 7.5.1, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an attacker who has already gained access to a victim's user account to reset the account credentials without being prompted for the account's password	6.8	More Details
CVE-2025-66237	DCIM dcTrack platforms utilize default and hard-coded credentials for access. An attacker could use these credentials to administer the database, escalate privileges on the platform or execute system commands on the host.	6.7	More Details
CVE-2025-40830	A vulnerability has been identified in SINEC Security Monitor (All versions < V4.10.0). The affected application does not have proper authorization checks for the file_transfer feature in ssmctl-client command. This could allow an authenticated, lowly privileged local attacker to read or write to any file on server or sensor.	6.7	More Details
CVE-2025-66326	Race condition vulnerability in the audio module. Impact: Successful exploitation of this vulnerability may affect availability.	6.7	More Details
CVE-2025-22432	In notifyTimeout of CallRedirectionProcessor.java, there is a possible persistent connection due to improper input validation. This could lead to local escalation of privilege and background activity launches with User execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2025-32319	In ensureBound of RemotePrintService.java, there is a possible way for a background app to keep foreground permissions due to a permissions bypass. This could lead to local escalation of privilege with user execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2025-46636	Dell Encryption, versions prior to 11.12.1, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	6.6	More Details
CVE-2024-47570	An insertion of sensitive information into log file vulnerability [CWE-532] in FortiOS 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0 all versions; FortiProxy 7.4.0 through 7.4.3, 7.2.0 through 7.2.11; FortiPAM 1.4 all versions, 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions and FortiSRA 1.4 all versions may allow a read-only administrator to retrieve API tokens of other administrators via observing REST API logs, if REST API logging is enabled (non-default configuration).	6.6	More Details
CVE-2025-48598	In multiple locations, there is a possible way to alter the primary user's face unlock settings due to a confused deputy. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	6.6	More Details
CVE-2025-42875	The SAP Internet Communication Framework does not conduct any authentication checks for features that need user identification allowing an attacker to reuse authorization tokens, violating secure authentication practices causing low impact on Confidentiality, Integrity and Availability of the application.	6.6	More Details
CVE-2025-63052	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GalleryCreator SimpLy Gallery simply-gallery-block allows Stored XSS.This issue affects SimpLy Gallery: from n/a through <= 3.2.8.	6.5	More Details
CVE-2025-66508	1Panel is an open-source, web-based control panel for Linux server management. Versions 2.0.14 and below use Gin's default configuration which trusts all IP addresses as proxies (TrustedProxies = 0.0.0.0/0), allowing any client to spoof the X-Forwarded-For header. Since all IP-based access controls (AllowIPs, API whitelists, localhost-only checks) rely on ClientIP(), attackers can bypass these protections by simply sending X-Forwarded-For: 127.0.0.1 or any whitelisted IP. This renders all IP-based security controls ineffective. This issue is fixed in version 2.0.14.	6.5	More Details
CVE-			

2025-41694	A low privileged remote attacker can run the webshell with an empty command containing whitespace. The server will then block until it receives more data, resulting in a DoS condition of the webserver.	6.5	More Details
CVE-2025-67535	Deserialization of Untrusted Data vulnerability in WePlugins - WordPress Development Company WP Maps wp-google-map-plugin allows Object Injection.This issue affects WP Maps: from n/a through <= 4.8.6.	6.5	More Details
CVE-2025-67536	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress learnpress allows Stored XSS.This issue affects LearnPress: from n/a through <= 4.2.9.4.	6.5	More Details
CVE-2025-40831	A vulnerability has been identified in SINEC Security Monitor (All versions < V4.10.0). The affected application lacks input validation of date parameter in report generation functionality. This could allow an authenticated, lowly privileged attacker to cause denial of service condition of the report functionality.	6.5	More Details
CVE-2025-36017	IBM Controller 11.1.0 through 11.1.1 and IBM Cognos Controller 11.0.0 through 11.0.1 FP6 stores unencrypted sensitive information in environmental variables files which can be obtained by an authenticated user.	6.5	More Details
CVE-2025-36015	IBM Controller 11.1.0 through 11.1.1 and IBM Cognos Controller 11.0.0 through 11.0.1 FP6 could allow an authenticated user to cause a denial of service due to improper validation of a specified quantity size input.	6.5	More Details
CVE-2025-61148	An Insecure Direct Object Reference (IDOR) vulnerability in the EduplusCampus 3.0.1 Student Payment API allows authenticated users to access other students personal and financial records by modifying the 'rec_no' parameter in the /student/get-receipt endpoint.	6.5	More Details
CVE-2025-64670	Exposure of sensitive information to an unauthorized actor in Microsoft Graphics Component allows an authorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-14206	A vulnerability was determined in SourceCodester Online Student Clearance System 1.0. The affected element is an unknown function of the file /Admin/delete-fee.php of the component Fee Table Handler. Executing manipulation of the argument ID can lead to improper authorization. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	6.5	More Details
CVE-2025-62465	Null pointer dereference in Windows DirectX allows an authorized attacker to deny service locally.	6.5	More Details
CVE-2025-57200	AVTECH SECURITY Corporation DGM1104 FullImg-1015-1004-1006-1003 was discovered to contain an authenticated command injection vulnerability in the test_mail function. This vulnerability allows attackers to execute arbitrary commands via a crafted input.	6.5	More Details
CVE-2025-14140	A vulnerability was detected in UTT 进取 520W 1.7.7-180627. The affected element is the function strcpy of the file /goform/websHostFilter. Performing manipulation of the argument addHostFilter results in buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2025-13359	The Tag, Category, and Taxonomy Manager – AI Autotagger with OpenAI plugin for WordPress is vulnerable to time-based SQL Injection via the "getTermsForAjax" function in all versions up to, and including, 3.40.1. This is due to insufficient escaping on the user supplied parameters 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 granted they have metabox access for the taxonomy (enabled by default for contributors).	6.5	More Details
CVE-2025-63075	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in muffingroup Betheme betheme allows DOM-Based XSS.This issue affects Betheme: from n/a through <= 28.1.7.	6.5	More Details
CVE-2025-63073	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dream-Theme The7 dt-the7 allows DOM-Based XSS.This issue affects The7: from n/a through <= 12.8.0.2.	6.5	More Details
CVE-2025-63072	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in THEMECO Cornerstone cornerstone allows Stored XSS.This issue affects Cornerstone: from n/a through <= 7.7.3.	6.5	More Details
CVE-2025-63066	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in p-themes Porto Theme - Functionality porto-functionality allows Stored XSS.This issue affects Porto Theme - Functionality: from n/a through <= 3.6.2.	6.5	More Details
CVE-2025-63064	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ashanjay EventON eventon allows Stored XSS.This issue affects EventON: from n/a through <= 4.9.12.	6.5	More Details
CVE-2025-13922	The Tag, Category, and Taxonomy Manager – AI Autotagger with OpenAI plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'existing_terms_orderby' parameter in the AI preview AJAX endpoint in all versions up to, and including, 3.40.1. This is due to insufficient escaping on user-supplied parameters and lack of SQL query parameterization. This makes it possible for authenticated attackers, with Contributor-level access and above who have AI metabox permissions, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database, cause performance degradation, or enable data inference through time-based techniques.	6.5	More Details
CVE-2025-59391	A memory disclosure vulnerability exists in libcoap's OSCORE configuration parser in libcoap before release-4.3.5-patches. An out-of-bounds read may occur when parsing certain configuration values, allowing an attacker to infer or read memory beyond string boundaries in the .rodata section. This could potentially lead to information disclosure or denial of service.	6.5	More Details
CVE-2025-65797	Incorrect access control in the Identity Provider service of usememos memos v0.25.2 allows attackers with low-level privileges to arbitrarily modify or delete registered identity providers, leading to an account takeover or Denial of Service (DoS).	6.5	More Details

CVE-2025-63063	Missing Authorization vulnerability in Yandex Metrika Yandex.Metrica wp-yandex-metrika allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Yandex.Metrica: from n/a through <= 1.2.2.	6.5	More Details
CVE-2025-63055	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liton Arefin Master Addons for Elementor master-addons allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through <= 2.0.9.9.	6.5	More Details
CVE-2025-63061	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hogash Kallyas kallyas allows DOM-Based XSS.This issue affects Kallyas: from n/a through <= 4.22.0.	6.5	More Details
CVE-2025-65900	Kalmia CMS version 0.2.0 contains an Incorrect Access Control vulnerability in the /kal-api/auth/users API endpoint. Due to insufficient permission validation and excessive data exposure in the backend, an authenticated user with basic read permissions can retrieve sensitive information for all platform users.	6.5	More Details
CVE-2025-67537	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Blair Williams ThirstyAffiliates thirstyaffiliates allows Stored XSS.This issue affects ThirstyAffiliates: from n/a through <= 3.11.8.	6.5	More Details
CVE-2025-62463	Null pointer dereference in Windows DirectX allows an authorized attacker to deny service locally.	6.5	More Details
CVE-2025-63046	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro listingpro-plugin allows DOM-Based XSS.This issue affects ListingPro: from n/a through <= 2.9.9.	6.5	More Details
CVE-2025-36140	IBM watsonx.data 2.2 through 2.2.1 could allow an authenticated user to cause a denial of service through ingestion pods due to improper allocation of resources without limits.	6.5	More Details
CVE-2025-64497	Tuleap is an Open Source Suite for management of software development and collaboration. Versions below 17.0.99.1762431347 of Tuleap Community Edition and Tuleap Enterprise Edition below 17.0-2, 16.13-7 and 16.12-10 allow attackers to access file release system information in projects they do not have access to. This issue is fixed in version 17.0.99.1762431347 of the Tuleap Community Edition and versions 17.0-2, 16.13-7 and 16.12-10 of Tuleap Enterprise Edition.	6.5	More Details
CVE-2025-66202	Astro is a web framework. Versions 5.15.7 and below have a double URL encoding bypass which allows any unauthenticated attacker to bypass path-based authentication checks in Astro middleware, granting unauthorized access to protected routes. While the original CVE-2025-64765 was fixed in v5.15.8, the fix is insufficient as it only decodes once. By using double-encoded URLs, attackers can still bypass authentication and access any route protected by middleware pathname checks. This issue is fixed in version 5.15.8.	6.5	More Details
CVE-2025-59810	An improper access control vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.2, FortiSOAR PaaS 7.5.0 through 7.5.1, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow information disclosure to an authenticated attacker via crafted requests	6.5	More Details
CVE-2025-63050	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sizam REHub Framework rehub-framework allows Stored XSS.This issue affects REHub Framework: from n/a through <= 19.9.8.	6.5	More Details
CVE-2025-63048	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro Lead Form listingpro-lead-form allows DOM-Based XSS.This issue affects ListingPro Lead Form: from n/a through <= 1.0.2.	6.5	More Details
CVE-2025-62473	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-65345	alexusmai laravel-file-manager 3.3.1 and below is vulnerable to Directory Traversal. The zip/archiving functionality allows an attacker to create archives containing files and directories outside the intended scope due to improper path validation.	6.5	More Details
CVE-2025-61727	An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.	6.5	More Details
CVE-2025-63059	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in arscode Ninja Popups arscode-ninja-popups allows Stored XSS.This issue affects Ninja Popups: from n/a through <= 4.7.8.	6.5	More Details
CVE-2025-67538	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jegtheme JNews Gallery jnews-gallery allows Stored XSS.This issue affects JNews Gallery: from n/a through < 12.0.1.	6.5	More Details
CVE-2025-67560	Missing Authorization vulnerability in Webilia Inc. Listdom listdom allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Listdom: from n/a through <= 5.0.1.	6.5	More Details
CVE-2025-67558	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jacques Malgrange Rencontre rencontre allows Stored XSS.This issue affects Rencontre: from n/a through <= 3.13.7.	6.5	More Details
CVE-2025-67544	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Get Bowtied Shopkeeper Extender shopkeeper-extender allows Stored XSS.This issue affects Shopkeeper Extender: from n/a through < 7.0.	6.5	More Details
CVE-2025-	Improper input validation in the Netconf service in Infinera MTC-9 allows remote authenticated users to crash the service and reboot the	6.5	More

26489	appliance, thus causing a DoS condition, via crafted XML payloads.This issue affects MTC-9: from R22.1.1.0275 before R23.0.		Details
CVE-2025-64527	Envoy is a high-performance edge/middle/service proxy. In 1.33.12, 1.34.10, 1.35.6, 1.36.2, and earlier, Envoy crashes when JWT authentication is configured with the remote JWKS fetching, allow_missing_or_failed is enabled, multiple JWT tokens are present in the request headers and the JWKS fetch fails. This is caused by a re-entry bug in the JwksFetcherImpl. When the first token's JWKS fetch fails, onJwksError() callback triggers processing of the second token, which calls fetch() again on the same fetcher object. The original callback's reset() then clears the second fetch's state (receiver_ and request_) which causes a crash when the async HTTP response arrives.	6.5	More Details
CVE-2025-65082	Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache HTTP Server through environment variables set via the Apache configuration unexpectedly superseding variables calculated by the server for CGI programs. This issue affects Apache HTTP Server from 2.4.0 through 2.4.65. Users are recommended to upgrade to version 2.4.66 which fixes the issue.	6.5	More Details
CVE-2025-67539	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Select-Themes Select Core select-core allows DOM-Based XSS.This issue affects Select Core: from n/a through < 2.6.	6.5	More Details
CVE-2025-14331	Same-origin policy bypass in the Request Handling component. This vulnerability affects Firefox < 146, Firefox ESR < 115.31, and Firefox ESR < 140.6.	6.5	More Details
CVE-2025-42904	Due to an Information Disclosure vulnerability in Application Server ABAP, an authenticated attacker could read unmasked values displayed in ABAP Lists. Successful exploitation could lead to unauthorized disclosure of data, resulting in a high impact on confidentiality without affecting integrity or availability.	6.5	More Details
CVE-2025-67540	Missing Authorization vulnerability in Wealcoder Animation Addons for Elementor animation-addons-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Animation Addons for Elementor: from n/a through <= 2.4.5.	6.5	More Details
CVE-2025-63037	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DFDevelopment Ronneby Theme Core ronneby-core allows DOM-Based XSS.This issue affects Ronneby Theme Core: from n/a through <= 1.5.68.	6.5	More Details
CVE-2025-63042	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Tutor LMS Elementor Addons tutor-lms-elementor-addons allows Stored XSS.This issue affects Tutor LMS Elementor Addons: from n/a through <= 3.0.1.	6.5	More Details
CVE-2025-63044	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons xpro-elementor-addons allows DOM-Based XSS.This issue affects Xpro Elementor Addons: from n/a through <= 1.4.19.1.	6.5	More Details
CVE-2025-65804	Tenda AX3 v16.03.12.11 contains a stack overflow in formSetIptv via the iptvType parameter, which can cause memory corruption and enable remote code execution (RCE).	6.5	More Details
CVE-2025-63045	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in averta Master Slider Pro masterslider allows DOM-Based XSS.This issue affects Master Slider Pro: from n/a through <= 3.7.12.	6.5	More Details
CVE-2025-64650	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.18 could disclose sensitive user credentials in log files.	6.5	More Details
CVE-2025-14254	Vitals ESP developed by Galaxy Software Services has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2025-14255	Vitals ESP developed by Galaxy Software Services has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2025-67542	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SilkyPress Multi-Step Checkout for WooCommerce wp-multi-step-checkout allows DOM-Based XSS.This issue affects Multi-Step Checkout for WooCommerce: from n/a through <= 2.33.	6.5	More Details
CVE-2025-67543	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Catch Themes Essential Widgets essential-widgets allows Stored XSS.This issue affects Essential Widgets: from n/a through <= 2.2.2.	6.5	More Details
CVE-2025-13898	The Ultra Skype Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'btn_id' parameter of the [ultra_skype] shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13896	The Social Feed Gallery Portfolio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the [igp-wp] shortcode in all versions up to, and including, 1.3 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-2025-13863	The RevInsite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `token` parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13899	The TR Timthumb plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcode attributes in all versions up to, and including, 1.0.4 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-	The Extra Post Images plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the extra-images		

2025-13856	shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13656	The Cute News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'color' shortcode attribute in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12717	The List Attachments Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before_list' parameter in the [list-attachments] shortcode in all versions up to, and including, 0.4.1a due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12715	The Canadian Nutrition Facts Label plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'percentage' field in the Nutrition Label custom post type in all versions up to, and including, 3.0 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-2025-13907	The CSS3 Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13857	The Yet Another WebClap for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' parameter of the webclap_button shortcode in all versions up to, and including, 0.2 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-2025-13448	The CSSIgniter Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'element' shortcode attribute in all versions up to, and including, 2.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13401	The Autoptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the LCP Image to preload metabox in all versions up to, and including, 3.1.13 due to insufficient input sanitization and output escaping on user-supplied image attributes in the "create_img_preload_tag" function. 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-2025-59788	Cross-site scripting (XSS) vulnerability in a reachable files_pdfviewer example directory in Nextcloud with versions before 22.2.10.33, 23.0.12.29, 24.0.12.28, 25.0.13.23, 26.0.13.20, 27.1.11.20, 28.0.14.11, 29.0.16.8, 30.0.17, 31.0.10, and 32.0.1 allows attackers to execute arbitrary JavaScript in the context of a user's browser via a crafted PDF file to viewer.html. This issue is related to CVE-2024-4367, but the root cause of this Nextcloud issue is that the product exposes executable example code on a same-origin basis.	6.4	More Details
CVE-2025-13739	The CryptX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `cryptx` shortcode in all versions up to, and including, 4.0.4 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-2025-13678	The Thai Lottery Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `thailottery` shortcode in all versions up to, and including, 2.5. This is due to insufficient input sanitization and output escaping on the user supplied `width` and `height` shortcode 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-2025-13860	The Easy Jump Links Menus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `h_tags` parameter in all versions up to, and including, 1.0.0 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-2025-12368	The Sermon Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `sermon-views` shortcode in all versions up to, and including, 2.30.0. 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-2025-12163	The Omnipress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2025-12417	The SurveyFunnel – Survey Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'surveyfunnel_lite_survey' shortcode in all versions up to, and including, 1.1.5 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-2025-12804	The Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin 'bookingcalendar' shortcode in all versions up to, and including, 10.14.6 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-2025-66404	MCP Server Kubernetes is an MCP Server that can connect to a Kubernetes cluster and manage it. Prior to 2.9.8, there is a security issue exists in the exec_in_pod tool of the mcp-server-kubernetes MCP Server. The tool accepts user-provided commands in both array and string formats. When a string format is provided, it is passed directly to shell interpretation (sh -c) without input validation, allowing shell metacharacters to be interpreted. This vulnerability can be exploited through direct command injection or indirect prompt injection attacks, where AI agents may execute commands without explicit user intent. This vulnerability is fixed in 2.9.8.	6.4	More Details
CVE-2025-14204	A vulnerability has been found in TykoDev cherry-studio-TykoFork 0.1. This issue affects the function redirectToAuthorization of the file /.well-known/oauth-authorization-server of the component OAuth Server Discovery. Such manipulation of the argument authorizationUrl leads to os command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-	A vulnerability was identified in Yonyou U8 Cloud 5.0/5.0sp/5.1/5.1sp. The affected element is an unknown function of the file		

2025-14185	nc/pubitf/erm/mobile/appservice/AppServletService.class. Such manipulation of the argument usercode leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-14214	A vulnerability has been found in itsourcecode Student Information System 1.0. This affects an unknown part of the file /section_edit1.php. The manipulation of the argument ID 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-2025-14089	A vulnerability was identified in Himool ERP up to 2.2. Affected by this issue is the function update_account of the file /api/admin/update_account/ of the component AdminActionViewSet. Such manipulation leads to improper authorization. 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-2025-14222	A flaw has been found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file /print_personnel_report.php. This manipulation of the argument per_id causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-14088	A vulnerability was determined in ketr JEPaaS up to 7.2.8. Affected by this vulnerability is an unknown functionality of the file /je/load. This manipulation of the argument Authorization causes improper authorization. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-14086	A vulnerability was found in youlaitech youlai-mall 1.0.0/2.0.0. Affected is an unknown function of the file /app-api/v1/members/openid/. The manipulation of the argument openid results in improper access controls. The attack can be executed remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-14085	A vulnerability has been found in youlaitech youlai-mall 1.0.0/2.0.0. This impacts an unknown function of the file /app-api/v1/orders/. The manipulation of the argument orderId leads to improper control of dynamically-identified variables. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-14182	A vulnerability has been found in Sobey Media Convergence System 2.0/2.1. This vulnerability affects unknown code of the file /sobey-mchEditor/watermark/upload. The manipulation of the argument File leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-14184	A vulnerability was determined in SGAI Space1 NAS N1211DS up to 1.0.915. Impacted is the function RENAME_FILE/OPERATE_FILE/NGNIX_UPLOAD of the file /cgi-bin/JSONAPI of the component gsaiagent. This manipulation causes command injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-40807	A vulnerability has been identified in Gridscale X Prepay (All versions < V4.2.1). The affected application is vulnerable to capture-replay of authentication tokens. This could allow an authenticated but already locked-out user to establish still valid user sessions.	6.3	More Details
CVE-2025-14227	A security flaw has been discovered in Philipinho Simple-PHP-Blog up to 94b5d3e57308bce5dfbc44c3edafa9811893d958. This issue affects some unknown processing of the file /edit.php. The manipulation results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-2848	A vulnerability in Synology Mail Server allows remote authenticated attackers to read and write non-sensitive settings, and disable some non-critical functions.	6.3	More Details
CVE-2025-14230	A vulnerability was detected in code-projects Daily Time Recording System 4.5.0. The impacted element is an unknown function of the file /admin/add_payroll.php. Performing manipulation of the argument detail_Id results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-14246	A vulnerability was found in code-projects Simple Shopping Cart 1.0. This vulnerability affects unknown code of the file /Customers/settings.php. Performing manipulation of the argument user_id results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-14259	A vulnerability was found in Jihai Jshop MiniProgram Mall System 2.9.0. Affected by this issue is some unknown functionality of the file /index.php/api.html. The manipulation of the argument cat_id results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-14247	A vulnerability was determined in code-projects Simple Shopping Cart 1.0. This issue affects some unknown processing of the file /Admin/additems.php. Executing manipulation of the argument item_name can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-14199	A flaw has been found in Verysync 微力同步 up to 2.21.3. This impacts an unknown function of the file /rest/f/api/resources/f96956469e7be39d/tmp/text.txt?override=false of the component Web Administration Module. Executing manipulation can lead to unrestricted upload. The attack may be performed from remote. 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-2025-14195	A security flaw has been discovered in code-projects Employee Profile Management System 1.0. Impacted is an unknown function of the file /profiling/add_file_query.php. The manipulation of the argument per_file results in unrestricted upload. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-66551	Nextcloud Tables allows you to create your own tables with individual columns. Prior to 0.8.6 and 0.9.3, a malicious user was able to create their own table and then move a column to a victims table. This vulnerability is fixed in 0.8.6 and 0.9.3.	6.3	More Details
CVE-2025-14052	A vulnerability has been found in youlaitech youlai-mall 1.0.0/2.0.0. Affected by this vulnerability is the function getMemberById of the file /mall-ums/app-api/v1/members/. The manipulation of the argument memberId leads to improper access controls. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
	A flaw has been found in youlaitech youlai-mall 1.0.0/2.0.0. Affected is the function getById/updateAddress/deleteAddress of the file /mall-		

CVE-2025-14051	ums/app-api/v1/addresses/. Executing manipulation can lead to improper control of dynamically-identified variables. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-14203	A flaw has been found in code-projects Question Paper Generator up to 1.0. This vulnerability affects unknown code of the file /selectquestionuser.php. This manipulation of the argument subid causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2025-14208	A security flaw has been discovered in D-Link DIR-823X up to 20250416. This affects the function sub_415028 of the file /goform/set_wan_settings. The manipulation of the argument ppp_username results in command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-14225	A vulnerability was determined in D-Link DCS-930L 1.15.04. This affects an unknown part of the file /setSystemAdmin of the component alphapd. Executing manipulation of the argument AdminID can lead to command injection. The attack can be executed remotely. 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-2025-14193	A vulnerability was determined in code-projects Employee Profile Management System 1.0. This vulnerability affects unknown code of the file /view_personnel.php. Executing manipulation of the argument per_id 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-2025-13949	A vulnerability was identified in ProudMuBai GoFilm 1.0.0/1.0.1. Impacted is the function SingleUpload of the file /server/controller/FileController.go. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-66325	Permission control vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2025-62686	A local privilege escalation vulnerability exists in the Plugin Alliance InstallationHelper service included with Plugin Alliance Installation Manager v1.4.0 on macOS. Due to the absence of a hardened runtime and a __RESTRICT segment, a local user may exploit the DYLD_INSERT_LIBRARIES environment variable to inject a dynamic library, potentially resulting in code execution with elevated privileges.	6.2	More Details
CVE-2025-65841	Aquarius Desktop 3.0.069 for macOS stores user authentication credentials in the local file ~/Library/Application Support/Aquarius/aquarius.settings using a weak obfuscation scheme. The password is "encrypted" through predictable byte-substitution that can be trivially reversed, allowing immediate recovery of the plaintext value. Any attacker who can read this settings file can fully compromise the victim's Aquarius account by importing the stolen configuration into their own client or login through the vendor website. This results in complete account takeover, unauthorized access to cloud-synchronized data, and the ability to perform authenticated actions as the user.	6.2	More Details
CVE-2025-55076	A local privilege escalation vulnerability exists in the InstallationHelper service included with Plugin Alliance Installation Manager v1.4.0 for macOS. The service accepts unauthenticated XPC connections and executes input via system(), which may allow a local user to execute arbitrary commands with root privileges.	6.2	More Details
CVE-2025-57202	A stored cross-site scripting (XSS) vulnerability in the PwdGrp.cgi endpoint of AVTECH SECURITY Corporation DGM1104 FullImg-1015-1004-1006-1003 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the username field.	6.1	More Details
CVE-2025-66470	NiceGUI is a Python-based UI framework. Versions 3.3.1 and below are subject to a XSS vulnerability through the ui.interactive_image component of NiceGUI. The component renders SVG content using Vue's v-html directive without any sanitization. This allows attackers to inject malicious HTML or JavaScript via the SVG <foreignObject> tag whenever the image component is rendered or updated. This is particularly dangerous for dashboards or multi-user applications displaying user-generated content or annotations. This issue is fixed in version 3.4.0.	6.1	More Details
CVE-2025-66469	NiceGUI is a Python-based UI framework. Versions 3.3.1 and below are vulnerable to Reflected XSS through its ui.add_css, ui.add_scss, and ui.add_sass functions. The functions lack proper sanitization or encoding for the JavaScript context they generate. An attacker can break out of the intended <style> or <script> tags by injecting closing tags (e.g., </style> or </script>), allowing for the execution of arbitrary JavaScript. This issue is fixed in version 3.4.0.	6.1	More Details
CVE-2025-14104	A flaw was found in util-linux. This vulnerability allows a heap buffer overread when processing 256-byte usernames, specifically within the `setpwnam()` function, affecting SUID (Set User ID) login-utils utilities writing to the password database.	6.1	More Details
CVE-2025-34409	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the Failed parameter of /Mondo/lang/sys/Forms/MAI/AddRecipientsResult.aspx. The Failed value is not properly sanitized when processed via a GET request and is reflected in the response, allowing an attacker to break out of existing markup and inject arbitrary script. A remote attacker can supply a crafted payload that closes an existing HTML list element, inserts attacker-controlled JavaScript, and comments out remaining code, leading to script execution in a victim’s browser when the victim visits a malicious link. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-41079	A stored Cross-Site Scripting (XSS) vulnerability has been found in Seafile v12.0.10. This vulnerability allows an attacker to execute arbitrary code in the victim's browser by storing malicious payloads with PUT parámetro 'name' in '/api/v2.1/user/'.	6.1	More Details
CVE-2025-34406	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the Id parameter of /Mobile/ContactDetails.aspx. The Id value is not properly sanitized when processed via a GET request and is reflected within a <script> block in the response. By supplying a crafted payload that terminates an existing JavaScript function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim’s browser when the victim opens a malicious link. Successful exploitation can redirect victims to malicious sites, steal cookies not protected by HttpOnly, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34397	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the Message parameter of /Mobile/Compose.aspx. The Message value is not properly sanitized when processed via a GET request and is reflected into a JavaScript context in the response. By supplying a crafted payload that terminates the existing script block/function, injects attacker-controlled JavaScript, and comments out the remaining code, a remote attacker can execute arbitrary JavaScript in a victim’s browser when the victim opens the crafted reply URL. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject	6.1	More Details

	arbitrary HTML or CSS, and perform actions as the authenticated user.		
CVE-2025-34398	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the AddressesBcc parameter of /Mondo/lang/sys/Forms/AddressBook.aspx. The AddressesBcc value is not properly sanitized when processed via a GET request and is reflected within a <script> block in the JavaScript variable var sAddrBcc. By supplying a crafted payload that terminates the existing LoadCurAddresses() function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser when the victim attempts to send an email. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34399	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the AddressesCc parameter of /Mondo/lang/sys/Forms/AddressBook.aspx. The AddressesCc value is not properly sanitized when processed via a GET request and is reflected within a <script> block in the JavaScript variable var sAddrCc. By supplying a crafted payload that terminates the existing LoadCurAddresses() function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser when the victim attempts to send an email. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34400	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the AddressesTo parameter of /Mondo/lang/sys/Forms/AddressBook.aspx. The AddressesTo value is not properly sanitized when processed via a GET request and is reflected within a <script> block in the response. By supplying a crafted payload that terminates the existing JavaScript function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser when the victim attempts to send an email. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34401	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the FieldBcc parameter of /Mondo/lang/sys/Forms/AddressBook.aspx. The FieldBcc value is not properly sanitized when processed via a GET request and is reflected inside a <script> block in the JavaScript variable var BCCFieldProvided. By supplying a crafted payload that terminates the existing LoadCurAddresses() function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser during normal email composition. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34402	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the FieldCc parameter of /Mondo/lang/sys/Forms/AddressBook.aspx. The FieldCc value is not properly sanitized when processed via a GET request and is reflected inside a <script> block in the JavaScript variable var CCFieldProvided. By supplying a crafted payload that terminates the existing LoadCurAddresses() function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser when the victim attempts to send an email. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34403	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the FieldTo parameter of /Mondo/lang/sys/Forms/AddressBook.aspx. The FieldTo value is not properly sanitized when processed via a GET request and is reflected inside a <script> block in the JavaScript variable var fieldTo. By supplying a crafted payload that terminates the existing Finish() function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser when the victim attempts to send an email. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34404	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the InstanceScope parameter of /Mondo/lang/sys/Forms/CAL/compose.aspx. The InstanceScope value is not properly sanitized when processed via a GET request and is reflected inside a <script> block in the JavaScript variable var gInstanceScope. By supplying a crafted payload that terminates the existing PageLoad() function, inserts attacker-controlled script, and comments out remaining code, a remote attacker can execute arbitrary JavaScript in a victim's browser. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-34407	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the theme parameter of /Mondo/lang/sys/Forms/Statistics.aspx. The theme value is insufficiently sanitized when processed via a GET request and is reflected in the response, allowing an attacker to break out of an existing iframe context and inject arbitrary script. A remote attacker can supply a crafted payload that closes the iframe tag, inserts attacker-controlled JavaScript, and comments out remaining code, leading to script execution in a victim's browser when the victim visits a malicious link. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-41080	A stored Cross-Site Scripting (XSS) vulnerability has been found in Seafile v12.0.10. This vulnerability allows an attacker to execute arbitrary code in the victim's browser by storing malicious payloads with POST parámetro 'p' in '/api/v2.1/repos/{repo_id}/file/'.	6.1	More Details
CVE-2025-34408	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the Added parameter of /Mondo/lang/sys/Forms/MAI/AddRecipientsResult.aspx. The Added value is not properly sanitized when processed via a GET request and is reflected in the response, allowing an attacker to break out of existing markup and inject arbitrary script. A remote attacker can supply a crafted payload that closes an existing HTML list element, inserts attacker-controlled JavaScript, and comments out remaining code, leading to script execution in a victim's browser when the victim visits a malicious link. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	6.1	More Details
CVE-2025-13512	The CoSign Single Signon plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 0.3.1 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-2025-13621	The dream gallery 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 on the 'dreampluginsmain' AJAX action. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-13622	The Jabbernotification plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the admin.php PATH_INFO in all versions up to, and including, 0.99-RC2 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-2025-13623	The Twitscription plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the admin.php PATH_INFO in all versions up to, and including, 0.1.1 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-2025-13625	The WP-SOS-Donate Donation Sidebar Plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 0.9.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13515	The Nouri.sh Newsletter plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 1.0.1.3 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-2025-11222	Central Dogma versions before 0.78.0 contain an Open Redirect vulnerability that allows attackers to redirect users to untrusted sites via specially crafted URLs, potentially facilitating phishing attacks and credential theft.	6.1	More Details
CVE-2025-14284	Versions of the package @tiptap/extension-link before 2.10.4 are vulnerable to Cross-site Scripting (XSS) due to unsanitized user input allowed in setting or toggling links. An attacker can execute arbitrary JavaScript code in the context of the application by injecting a javascript: URL payload into these attributes, which is then triggered either by user interaction.	6.1	More Details
CVE-2025-13513	The Clik stats plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13137	The Live Sales Notification for Woocommerce – Woomotiv plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'woomotiv_limit' parameter in all versions up to, and including, 3.6.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13626	The myLCO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 0.8.1 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-2025-11263	The Link Whisper Free plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the type parameter in all versions up to, and including, 0.8.8 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-2025-65516	A stored cross-site scripting (XSS) vulnerability was discovered in Seafile Community Edition prior to version 13.0.12. When Seafile is configured with the Golang file server, an attacker can upload a crafted SVG file containing malicious JavaScript and share it using a public link. Opening the link triggers script execution in the victim's browser. This issue has been fixed in Seafile Community Edition 13.0.12.	6.1	More Details
CVE-2025-63499	Alinto Sogo 5.12.3 is vulnerable to Cross Site Scripting (XSS) via the theme parameter.	6.1	More Details
CVE-2025-42872	Due to a Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal, an unauthenticated attacker could inject malicious scripts that execute in the context of other users browsers, allowing the attacker to steal session cookies, tokens, and other sensitive information. As a result, the vulnerability has a low impact on confidentiality and integrity and no impact on availability.	6.1	More Details
CVE-2025-13894	The CSV Sumotto plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.0 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-2025-66578	xmlseclibs is a library written in PHP for working with XML Encryption and Signatures. Versions 3.1.3 contain an authentication bypass vulnerability due to a flaw in the libxml2 canonicalization process during document transformation. When libxml2's canonicalization is invoked on an invalid XML input, it may return an empty string rather than a canonicalized node. xmlseclibs then proceeds to compute the DigestValue over this empty string, treating it as if canonicalization succeeded. This issue is fixed in version 3.1.4. Workarounds include treating canonicalization failures (exceptions or nil/empty outputs) as fatal and aborting validation, and/or adding explicit checks to reject when canonicalize returns nil/empty or raises errors.	6.0	More Details
CVE-2025-42873	SAPUI5 (and OpenUI5) packages use outdated 3rd party libraries with known security vulnerabilities. When markdown-it encounters special malformed input, it fails to terminate properly, resulting in an infinite loop. This Denial of Service via infinite loop causes high CPU usage and system unresponsiveness due to a blocked processing thread. This vulnerability has no impact on confidentiality or integrity but has a high impact on system availability.	5.9	More Details
CVE-2025-66491	Traefik is an HTTP reverse proxy and load balancer. Versions 3.5.0 through 3.6.2 have inverted TLS verification logic in the nginx.ingress.kubernetes.io/proxy-ssl-verify annotation. Setting the annotation to "on" (intending to enable backend TLS certificate verification) actually disables verification, allowing man-in-the-middle attacks against HTTPS backends when operators believe they are protected. This issue is fixed in version 3.6.3.	5.9	More Details
CVE-2025-62408	c-ares is an asynchronous resolver library. Versions 1.32.3 through 1.34.5 terminate a query after maximum attempts when using read_answer() and process_answer(), which can cause a Denial of Service. This issue is fixed in version 1.34.6.	5.9	More Details
CVE-2025-63361	Waveshare RS232/485 TO WIFI ETH (B) Serial to Ethernet/Wi-Fi Gateway Firmware V3.1.1.0: HW 4.3.2.1: Webpage V7.04T.07.002880.0301 was discovered to render the Administrator password in plaintext.	5.7	More Details
CVE-2025-14139	A security vulnerability has been detected in UTT 进取 520W 1.7.7-180627. Impacted is the function strcpy of the file /goform/formConfigDnsFilterGlobal. Such manipulation of the argument timeRangeName leads to buffer overflow. 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.	5.7	More Details
CVE-2025-66550	Nextcloud Calendar is a calendar app for Nextcloud. Prior to 4.7.17 and 5.2.4, when a malicious user creates a calendar event with a crafted attachment that links to a download link of a file on the same Nextcloud server, the file would be downloaded without the user confirming the action. This vulnerability is fixed in 4.7.17 and 5.2.4.	5.7	More Details
CVE-2025-62631	An insufficient session expiration vulnerability [CWE-613] in Fortinet FortiOS 7.4.0, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions allows attacker to maintain access to network resources via an active SSLVPN session not terminated after a user's password change under particular conditions outside of the attacker's control	5.6	More Details

CVE-2025-13948	A vulnerability was determined in opsre go-ldap-admin up to 20251011. This issue affects some unknown processing of the file docs/docker-compose/docker-compose.yaml of the component JWT Handler. Executing manipulation of the argument secret key can lead to use of hard-coded cryptographic key . The attack can be launched remotely. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The exploit has been publicly disclosed and may be utilized.	5.6	More Details
CVE-2025-14276	A vulnerability was determined in Ilevia EVE X1 Server up to 4.6.5.0.eden. Impacted is an unknown function of the file /ajax/php/leaf_search.php. This manipulation of the argument line causes command injection. The attack can be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is considered difficult. The exploit has been publicly disclosed and may be utilized. Upgrading the affected component is recommended. The vendor confirms the issue and recommends: "We already know that issue and on most devices are already solved, also it’s not needed to open the port to outside world so we advised our customer to close it".	5.6	More Details
CVE-2025-8074	Origin validation error vulnerability in BeeDrive in Synology BeeDrive for desktop before 1.4.3-13973 allows local users to write arbitrary files with non-sensitive information via unspecified vectors.	5.6	More Details
CVE-2025-13945	HTTP3 dissector crash in Wireshark 4.6.0 and 4.6.1 allows denial of service	5.5	More Details
CVE-2025-48601	In multiple locations, there is a possible permanent denial of service due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48610	In __pkvm_guest_relinquish_to_host of mem_protect.c, there is a possible configuration data leak due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-13946	MEGACO dissector infinite loop in Wireshark 4.6.0 to 4.6.1 and 4.4.0 to 4.4.11 allows denial of service	5.5	More Details
CVE-2025-42891	Due to a missing authorization check in SAP Enterprise Search for ABAP, an attacker with high privileges may read and export the contents of database tables into an ABAP report. This could lead to a high impact on data confidentiality and a low impact on data integrity. There is no impact on application's availability.	5.5	More Details
CVE-2025-48607	In multiple locations, there is a possible way to create a large amount of app ops due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48590	In verifyAndGetBypass of AppOpsService.java, there is a possible method for a malicious app to prevent dialing emergency services under limited circumstances due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48591	In multiple locations, there is a possible way to read files from another user due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-14010	A flaw was found in ansible-collection-community-general. This vulnerability allows for information exposure (IE) of sensitive credentials, specifically plaintext passwords, via verbose output when running Ansible with debug modes. Attackers with access to logs could retrieve these secrets and potentially compromise Keycloak accounts or administrative access.	5.5	More Details
CVE-2025-48584	In multiple functions of NotificationManagerService.java, there is a possible way to bypass the per-package channel limits causing resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48622	In ProcessArea of dng_misc_opcodes.cpp, there is a possible out of bounds read due to a buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-64896	Creative Cloud Desktop versions 6.4.0.361 and earlier are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to disrupt the application's functionality by manipulating temporary files. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-64894	DNG SDK versions 1.7.0 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could lead to application denial-of-service. An attacker could exploit this issue to cause the application to crash or become unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-48633	In hasAccountsOnAnyUser of DevicePolicyManagerService.java, there is a possible way to add a Device Owner after provisioning due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48600	In multiple files, there is a possible way to reveal information across users due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48576	In updateNotificationChannelGroupFromPrivilegedListener of NotificationManagerService.java, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48608	In isValidMediaUri of SettingsProvider.java, there is a possible cross user media read due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-63401	Cross Site Scripting vulnerability in HCL Technologies Limited HCLTech DRAGON before v.7.6.0 allows a remote attacker to execute arbitrary code via missing directives	5.5	More Details

CVE-2025-63402	An issue in HCL Technologies Limited HCLTech GRAGON before v.7.6.0 allows a remote attacker to execute arbitrary code via APIs do not enforcing limits on the number or size of requests	5.5	More Details
CVE-2025-48603	In InputMethodInfo of InputMethodInfo.java, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48604	In multiple locations, there is a possible way to read files from another user due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-48569	In multiple locations, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2025-66200	mod_userdir+suexec bypass via AllowOverride FileInfo vulnerability in Apache HTTP Server. Users with access to use the RequestHeader directive in htaccess can cause some CGI scripts to run under an unexpected userid. This issue affects Apache HTTP Server: from 2.4.7 through 2.4.65. Users are recommended to upgrade to version 2.4.66, which fixes the issue.	5.4	More Details
CVE-2025-20381	In Splunk MCP Server app versions below 0.2.4, a user with access to the "run_splunk_query" Model Context Protocol (MCP) tool could bypass the SPL command allowlist controls in MCP by embedding SPL commands as sub-searches, leading to unauthorized actions beyond the intended MCP restrictions.	5.4	More Details
CVE-2025-67559	Missing Authorization vulnerability in vcita Online Booking & Scheduling Calendar for WordPress by vcita meeting-scheduler-by-vcita allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through <= 4.5.5.	5.4	More Details
CVE-2025-67561	Missing Authorization vulnerability in Oleksandr Lysyi Debug Log Viewer debug-log-viewer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Debug Log Viewer: from n/a through <= 2.0.3.	5.4	More Details
CVE-2023-23729	Missing Authorization vulnerability in Brainstorm Force Spectra allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Spectra: from n/a through 2.3.0.	5.4	More Details
CVE-2025-65798	Incorrect access control in usememos memos v0.25.2 allows attackers with low-level privileges to arbitrarily modify or delete attachments made by other users.	5.4	More Details
CVE-2025-13308	The Application Passwords plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'reject_url' parameter in all versions up to, and including, 0.1.3. This is due to insufficient input sanitization and output escaping on user supplied URLs, which allows javascript: URI schemes to be embedded in the reject_url parameter. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when a user clicks the "No, I do not approve of this connection" button, granted they can successfully trick the victim into performing an action such as clicking on a link.	5.4	More Details
CVE-2025-12887	The Post SMTP plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.6.1. This is due to the plugin not properly verifying that a user is authorized to update OAuth tokens on the 'handle_gmail_oauth_redirect' function. This makes it possible for authenticated attackers, with subscriber level access and above, to inject invalid or attacker-controlled OAuth credentials.	5.4	More Details
CVE-2025-13642	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 4.16.7 due to insufficient input sanitization on the `type` parameter in the form preview functionality. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes via the `pp_preview_form` endpoint.	5.4	More Details
CVE-2025-54353	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.0 through 4.4.7, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may allow an attacker to perform an XSS attack via crafted HTTP requests.	5.4	More Details
CVE-2025-63065	Authorization Bypass Through User-Controlled Key vulnerability in David Lingren Media Library Assistant media-library-assistant allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Media Library Assistant: from n/a through <= 3.30.	5.4	More Details
CVE-2025-66512	Nextcloud Server is a self hosted personal cloud system. In Nextcloud Server and Server Enterprise prior to 31.0.12 and 32.0.3, a missing sanitization allowed malicious users to circumvent the content security policy when a malicious user manages to trick a user it viewing an uploaded SVG outside of the Nextcloud Servers web page.	5.4	More Details
CVE-2025-29843	A vulnerability in FileStation thumb cgi allows remote authenticated users to read/write image files.	5.4	More Details
CVE-2025-12191	The PDF Catalog for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pdfcatalog' AJAX action in all versions up to, and including, 1.1.18 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-66557	Nextcloud Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. Prior to 1.14.6 and 1.15.2, a bug in the permission logic allowed users with "Can share" permission to modify the permissions of other recipients. This vulnerability is fixed in 1.14.6 and 1.15.2.	5.4	More Details
CVE-2025-12505	The weDocs plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 2.1.14. This is due to the plugin not properly verifying that a user is authorized to perform an action in the create_item_permissions_check function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify global plugin settings.	5.4	More Details
CVE-2025-14016	A security vulnerability has been detected in macrozheng mall-swarm up to 1.0.3. Affected is the function delete of the file /member/readHistory/delete. Such manipulation of the argument ids leads to improper authorization. The attack can be executed 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.	5.4	More Details

CVE-2025-42896	SAP BusinessObjects Business Intelligence Platform lets an unauthenticated remote attacker send crafted requests through the URL parameter that controls the login page error message. This can cause the server to fetch attacker-supplied URLs, resulting in low impact to confidentiality and integrity, and no impact to availability.	5.4	More Details
CVE-2025-6924	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TalentSoft Software e-BAP Automation allows Reflected XSS.This issue affects e-BAP Automation: before 42957.	5.4	More Details
CVE-2025-12635	IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.12 are affected by cross-site scripting due to improper validation of user-supplied input. An attacker could exploit this vulnerability by using a specially crafted URL to redirect the user to a malicious site.	5.4	More Details
CVE-2025-6923	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TalentSoft Software UNIS allows Reflected XSS.This issue affects UNIS: before 42957.	5.4	More Details
CVE-2025-67578	Missing Authorization vulnerability in Rhys Wynne WP Email Capture wp-email-capture allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Email Capture: from n/a through <= 3.12.4.	5.3	More Details
CVE-2025-67577	Missing Authorization vulnerability in hassantafreshi Easy Form Builder easy-form-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Form Builder: from n/a through <= 3.8.20.	5.3	More Details
CVE-2025-67579	Missing Authorization vulnerability in vanquish User Extra Fields wp-user-extra-fields allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Extra Fields: from n/a through <= 16.8.	5.3	More Details
CVE-2025-67574	Missing Authorization vulnerability in wpdevart Booking calendar, Appointment Booking System booking-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booking calendar, Appointment Booking System: from n/a through <= 3.2.30.	5.3	More Details
CVE-2025-67576	Missing Authorization vulnerability in QuantumCloud Simple Link Directory simple-link-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simple Link Directory: from n/a through <= 8.8.3.	5.3	More Details
CVE-2025-67580	Missing Authorization vulnerability in Constant Contact Constant Contact + WooCommerce constant-contact-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Constant Contact + WooCommerce: from n/a through <= 2.4.1.	5.3	More Details
CVE-2025-67575	Missing Authorization vulnerability in Andrew Lima Sitewide Notice WP sitewide-notice-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sitewide Notice WP: from n/a through <= 2.4.1.	5.3	More Details
CVE-2025-67586	Missing Authorization vulnerability in Ronald Huereca Highlight and Share highlight-and-share allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Highlight and Share: from n/a through <= 5.2.0.	5.3	More Details
CVE-2025-67581	Missing Authorization vulnerability in themetechmount TrueBooker truebooker-appointment-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TrueBooker: from n/a through <= 1.1.0.	5.3	More Details
CVE-2025-11379	The WebP Express plugin for WordPress is vulnerable to information exposure via config files in all versions up to, and including, 0.25.9. This is due to the plugin not properly randomizing the name of the config file to prevent direct access on NGINX. This makes it possible for unauthenticated attackers to extract configuration data.	5.3	More Details
CVE-2025-67582	Missing Authorization vulnerability in wbcomdesigns Wbcom Designs lock-my-bp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wbcom Designs: from n/a through <= 2.1.1.	5.3	More Details
CVE-2025-67583	Missing Authorization vulnerability in ThemeAtelier IDonate idonate allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects IDonate: from n/a through <= 2.1.15.	5.3	More Details
CVE-2025-67584	Missing Authorization vulnerability in rtCamp GoDAM godam allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GoDAM: from n/a through <= 1.4.6.	5.3	More Details
CVE-2025-13528	The Feedback Modal for Website plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'handle_export' function in all versions up to, and including, 1.0.1. This makes it possible for unauthenticated attackers to export all feedback data in CSV or JSON format via the 'export_data' parameter.	5.3	More Details
CVE-2025-12585	The MxChat – AI Chatbot for WordPress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.5.5 via upload filenames. This makes it possible for unauthenticated attackers to extract session values that can subsequently be used to access conversation data.	5.3	More Details
CVE-2025-66323	Vulnerability of improper criterion security check in the card module. Impact: Successful exploitation of this vulnerability may affect availability.	5.3	More Details
CVE-2025-13620	The Wp Social Login and Register Social Counter plugin for WordPress is vulnerable to missing authorization in versions up to, and including, 3.1.3. This is due to the REST routes wslu/v1/check_cache/{type}, wslu/v1/save_cache/{type}, and wslu/v1/settings/clear_counter_cache being registered with permission_callback set to __return_true and lacking capability or nonce validation in their handlers. This makes it possible for unauthenticated attackers to clear or overwrite the social counter cache via crafted REST requests.	5.3	More Details
CVE-2025-	The Voidek Employee Portal plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several AJAX actions in all versions up to, and including, 1.0.6. This makes it possible for unauthenticated attackers to perform several actions like	5.3	More

12093	registering an account, deleting users, and modifying details within the employee portal.		Details
CVE-2025-12355	The Payaza plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_nopriv_update_order_status' AJAX endpoint in all versions up to, and including, 0.3.8. This makes it possible for unauthenticated attackers to update order statuses.	5.3	More Details
CVE-2025-12720	The g-FFL Cockpit plugin for WordPress is vulnerable to unauthorized modification of data due to IP-based authorization that can be spoofed in the handle_enqueue_only() function in all versions up to, and including, 1.7.1. This makes it possible for unauthenticated attackers to delete arbitrary products.	5.3	More Details
CVE-2025-13358	The Accessiy By CodeConfig Accessibility plugin for WordPress is vulnerable to unauthorized page creation due to missing authorization checks in versions up to, and including, 1.0.0. This is due to the plugin not performing capability checks in the `Settings::createPage()` function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary published pages on the site via the `ccpcaCreatePage` AJAX action.	5.3	More Details
CVE-2025-12876	The Projectopia – WordPress Project Management plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pto_delete_file AJAX action in all versions up to, and including, 5.1.19. This makes it possible for unauthenticated attackers to delete arbitrary attachments.	5.3	More Details
CVE-2025-12721	The g-FFL Cockpit plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.7.1 via the /server_status REST API endpoint due to a lack of capability checks. This makes it possible for unauthenticated attackers to extract information about the server.	5.3	More Details
CVE-2025-67567	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in uixthemes Sober sober allows Retrieve Embedded Sensitive Data.This issue affects Sober: from n/a through <= 3.5.11.	5.3	More Details
CVE-2025-13666	The Helloprint plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.1.2. This is due to the plugin registering a public REST API endpoint without implementing authorization checks to verify request authenticity. This makes it possible for unauthenticated attackers to arbitrarily modify WooCommerce order statuses via the /wp-json/helloprint/v1/complete_order_from_helloprint_callback endpoint by providing a valid order reference ID.	5.3	More Details
CVE-2025-67566	Missing Authorization vulnerability in WofficeIO Woffice Core woffice-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Woffice Core: from n/a through <= 5.4.30.	5.3	More Details
CVE-2025-14197	A security vulnerability has been detected in Verysync 微力同步 up to 2.21.3. The impacted element is an unknown function of the file /rest/f/api/resources/f96956469e7be39d of the component Web Administration Module. Such manipulation leads to information disclosure. The attack can be executed 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.	5.3	More Details
CVE-2025-63071	Insertion of Sensitive Information Into Sent Data vulnerability in averta Shortcodes and extra features for Phlox theme auxin-elements allows Retrieve Embedded Sensitive Data.This issue affects Shortcodes and extra features for Phlox theme: from n/a through <= 2.17.12.	5.3	More Details
CVE-2025-63069	Missing Authorization vulnerability in Vinod Dalvi Ivory Search add-search-to-menu allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ivory Search: from n/a through <= 5.5.12.	5.3	More Details
CVE-2025-63068	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in sevenspark Contact Form 7 Dynamic Text Extension contact-form-7-dynamic-text-extension allows Code Injection.This issue affects Contact Form 7 Dynamic Text Extension: from n/a through <= 5.0.3.	5.3	More Details
CVE-2025-10876	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TalentSoft Software e-BAP Automation allows Cross-Site Scripting (XSS).This issue affects e-BAP Automation: from 1.8.96 before v.41815.	5.3	More Details
CVE-2025-62567	Integer underflow (wrap or wraparound) in Windows Hyper-V allows an authorized attacker to deny service over a network.	5.3	More Details
CVE-2025-10304	The Everest Backup – WordPress Cloud Backup, Migration, Restore & Cloning Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the process_status_unlink() function in all versions up to, and including, 2.3.8. This makes it possible for unauthenticated attackers to delete the back-up progress files and cause a back-up to fail while it is in progress.	5.3	More Details
CVE-2025-12994	Medtronic CareLink Network allows an unauthenticated remote attacker to initiate a request for security questions to an API endpoint that could be used to determine a valid user account. This issue affects CareLink Network: before December 4, 2025.	5.3	More Details
CVE-2025-14198	A vulnerability was detected in Verysync 微力同步 2.21.3. This affects an unknown function of the file /safebrowsing/clientreport/download?key=dummytoken of the component Web Administration Module. Performing manipulation results in information disclosure. The attack is possible to be carried out 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-2025-66577	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.27.0, a vulnerability allows attacker-controlled HTTP headers to influence server-visible metadata, logging, and authorization decisions. An attacker can supply X-Forwarded-For or X-Real-IP headers which get accepted unconditionally by get_client_ip() in docker/main.cc, causing access and error logs (nginx_access_logger / nginx_error_logger) to record spoofed client IPs (log poisoning / audit evasion). This vulnerability is fixed in 0.27.0.	5.3	More Details
CVE-2025-13312	The CRM Memberships plugin for WordPress is vulnerable to unauthorized membership tag creation due to a missing capability check on the 'ntzcrm_add_new_tag' function in all versions up to, and including, 2.5. This makes it possible for unauthenticated attackers to create arbitrary membership tags and modify CRM configuration that should be restricted to administrators.	5.3	More Details
CVE-2025-59029	An attacker can trigger an assertion failure by requesting crafted DNS records, waiting for them to be inserted into the records cache, then send a query with qtype set to ANY.	5.3	More Details

CVE-2025-65899	Kalmia CMS version 0.2.0 contains a user enumeration vulnerability in its authentication mechanism. The application returns different error messages for invalid users (user_not_found) versus valid users with incorrect passwords (invalid_password). This observable response discrepancy allows unauthenticated attackers to enumerate valid usernames on the system.	5.3	More Details
CVE-2022-46845	Missing Authorization vulnerability in Essential Plugin Slider a SlidersPack allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Slider a SlidersPack: from n/a before 2.3.	5.3	More Details
CVE-2025-14286	A vulnerability was determined in Tenda AC9 15.03.05.14_multi. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/DownloadCfg.jpg of the component Configuration File Handler. This manipulation causes information disclosure. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	5.3	More Details
CVE-2025-63054	Missing Authorization vulnerability in ExpressTech Systems Quiz And Survey Master quiz-master-next allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Quiz And Survey Master: from n/a through <= 10.3.1.	5.3	More Details
CVE-2025-63049	Missing Authorization vulnerability in CridioStudio ListingPro Lead Form listingpro-lead-form allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects ListingPro Lead Form: from n/a through <= 1.0.2.	5.3	More Details
CVE-2025-63047	Missing Authorization vulnerability in CridioStudio ListingPro listingpro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ListingPro: from n/a through <= 2.9.9.	5.3	More Details
CVE-2025-40806	A vulnerability has been identified in Gridscale X Prepay (All versions < V4.2.1). The affected application is vulnerable to user enumeration due to distinguishable responses. This could allow an unauthenticated remote attacker to determine if a user is valid or not, enabling a brute force attack with valid users.	5.3	More Details
CVE-2025-13006	The SurveyFunnel – Survey Plugin for WordPress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.5 via several unprotected /wp-json/surveyfunnel/v2/ REST API endpoints. This makes it possible for unauthenticated attackers to extract sensitive data from survey responses.	5.3	More Details
CVE-2025-53965	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. The function used to decode the SOR transparent container lacks bounds checking, which can cause a fatal error.	5.3	More Details
CVE-2025-67562	Missing Authorization vulnerability in WebCodingPlace Image Caption Hover Pro image-caption-hover-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Caption Hover Pro: from n/a through < 20.0.	5.3	More Details
CVE-2025-67565	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in sizam Rehub rehub-theme allows Retrieve Embedded Sensitive Data.This issue affects Rehub: from n/a through <= 19.9.9.1.	5.3	More Details
CVE-2025-13494	The SSP Debug plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.0. This is due to the plugin storing PHP error logs in a predictable, web-accessible location (wp-content/uploads/ssp-debug/ssp-debug.log) without any access controls. This makes it possible for unauthenticated attackers to view sensitive debugging information including full URLs, client IP addresses, User-Agent strings, WordPress user IDs, and internal filesystem paths.	5.3	More Details
CVE-2025-67563	Missing Authorization vulnerability in Saad Iqbal Post SMTP post-smtp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post SMTP: from n/a through <= 3.6.1.	5.3	More Details
CVE-2025-20384	In Splunk Enterprise versions below 10.0.1, 9.4.6, 9.3.8, and 9.2.10, and Splunk Cloud Platform versions below 10.1.2507.4, 10.0.2503.6, and 9.3.2411.117.125, an unauthenticated attacker can inject American National Standards Institute (ANSI) escape codes into Splunk log files due to improper validation at the /en-US/static/ web endpoint. This may allow them to poison, forge, or obfuscate sensitive log data through specially crafted HTTP requests, potentially impacting log integrity and detection capabilities.	5.3	More Details
CVE-2025-67564	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in alekv Pixel Manager for WooCommerce woocommerce-google-adwords-conversion-tracking-tag allows Retrieve Embedded Sensitive Data.This issue affects Pixel Manager for WooCommerce: from n/a through <= 1.51.1.	5.3	More Details
CVE-2025-64667	User interface (ui) misrepresentation of critical information in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	5.3	More Details
CVE-2025-13748	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.1.7 via the 'submission_id' parameter due to missing validation on a user controlled key within the confirmScaPayment() function. This makes it possible for unauthenticated attackers to mark arbitrary submissions as failed via crafted requests to the endpoint granted they can guess or enumerate a valid submission identifier.	5.3	More Details
CVE-2025-67528	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Urna urna allows PHP Local File Inclusion.This issue affects Urna: from n/a through <= 2.5.12.	5.1	More Details
CVE-2025-66322	Multi-thread race condition vulnerability in the camera framework module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2025-66321	Multi-thread race condition vulnerability in the camera framework module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2025-66320	Multi-thread race condition vulnerability in the camera framework module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
	The Aquarius HelperTool (1.0.003) privileged XPC service on macOS contains multiple flaws that allow local privilege escalation. The		

CVE-2025-65842	service accepts XPC connections from any local process without validating the client's identity, and its authorization logic incorrectly calls AuthorizationCopyRights with a NULL reference, causing all authorization checks to succeed. The executeCommand:authorization:withReply: method then interpolates attacker-controlled input into NSTask and executes it with root privileges. A local attacker can exploit these weaknesses to run arbitrary commands as root, create persistent backdoors, or obtain a fully interactive root shell.	5.1	More Details
CVE-2025-64052	An issue was discovered in Fanvil x210 V2 2.12.20 allowing unauthenticated attackers on the local network to execute arbitrary system commands.	5.1	More Details
CVE-2025-50361	Buffer Overflow was found in SmallBASIC community SmallBASIC with SDL Before v12_28, and commit sha:298a1d495355959db36451e90a0ac74bcc5593fe in the function main.cpp, which can lead to potential information leakage and crash.	5.1	More Details
CVE-2025-66220	Envoy is a high-performance edge/middle/service proxy. In 1.33.12, 1.34.10, 1.35.6, 1.36.2, and earlier, Envoy’s mTLS certificate matcher for match_typed_subject_alt_names may incorrectly treat certificates containing an embedded null byte (\0) inside an OTHERNAME SAN value as valid matches.	5.0	More Details
CVE-2025-66406	Step CA is an online certificate authority for secure, automated certificate management for DevOps. Prior to 0.29.0, there is an improper authorization check for SSH certificate revocation. This affects deployments configured with the SSHPOP provisioner. This vulnerability is fixed in 0.29.0.	5.0	More Details
CVE-2025-14111	A security vulnerability has been detected in Rarlab RAR App up to 7.11 Build 127 on Android. This affects an unknown part of the component com.rarlab.rar. Such manipulation leads to path traversal. It is possible to launch the attack remotely. Attacks of this nature are highly complex. It is indicated that the exploitability is difficult. The exploit has been disclosed publicly and may be used. Upgrading to version 7.20 build 128 is able to mitigate this issue. You should upgrade the affected component. The vendor responded very professional: "This is the real vulnerability affecting RAR for Android only. WinRAR and Unix RAR versions are not affected. We already fixed it in RAR for Android 7.20 build 128 and we publicly mentioned it in that version changelog. (...) To avoid confusion among users, it would be useful if such disclosure emphasizes that it is RAR for Android only issue and WinRAR isn't affected."	5.0	More Details
CVE-2016-20023	In CKSource CKFinder before 2.5.0.1 for ASP.NET, authenticated users could download any file from the server if the correct path to a file was provided.	5.0	More Details
CVE-2025-64471	A use of password hash instead of password for authentication vulnerability [CWE-836] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.4, FortiWeb 7.4.0 through 7.4.10, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow an unauthenticated attacker to use the hash in place of the password to authenticate via crafted HTTP/HTTPS requests	4.9	More Details
CVE-2025-66330	App lock verification bypass vulnerability in the file management app. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.9	More Details
CVE-2025-13495	The FluentCart plugin for WordPress is vulnerable to SQL Injection via the 'groupKey' parameter in all versions up to, and including, 1.3.1. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-14253	Vitals ESP developed by Galaxy Software Services has an Arbitrary File Read vulnerability, allowing privileged remote attackers to exploit Absolute Path Traversal to download arbitrary system files.	4.9	More Details
CVE-2025-40940	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected application exhibits inconsistent SNMP behavior, such as unexpected service availability and unreliable configuration handling across protocol versions. This could allow an attacker to access sensitive data, potentially leading to a breach of confidentiality.	4.9	More Details
CVE-2025-66625	Umbraco is an ASP.NET CMS. Due to unsafe handling and deletion of temporary files in versions 10.0.0 through 13.12.0, during the dictionary upload process an attacker with access to the backoffice can trigger predictable requests to temporary file paths. The application’s error responses (HTTP 500 when a file exists, 404 when it does not) allow the attacker to enumerate the existence of arbitrary files on the server’s filesystem. This vulnerability does not allow reading or writing file contents. In certain configurations, incomplete clean-up of temporary upload files may additionally expose the NTLM hash of the Windows account running the Umbraco application. This issue is fixed in version 13.12.1.	4.9	More Details
CVE-2025-12826	The Custom Post Type UI plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.18.0. This is due to the plugin not verifying that a user has the required capability to perform actions in the "cptui_process_post_type" function. This makes it possible for authenticated attackers, with subscriber level access and above, to add, edit, or delete custom post types in limited situations.	4.8	More Details
CVE-2025-66511	Nextcloud Calendar is a calendar app for Nextcloud. Prior to 6.0.3, the Calendar app generates participant tokens for meeting proposals using a hash function, allowing an attacker to compute valid participant tokens, which allowed them to request details and submit dates in meeting proposals. The tokens are not purely random generated. This vulnerability is fixed in 6.0.3.	4.8	More Details
CVE-2025-66373	Akamai Ghost on Akamai CDN edge servers before 2025-11-17 has a chunked request body processing error that can result in HTTP request smuggling. When Akamai Ghost receives an invalid chunked body that includes a chunk size different from the actual size of the following chunk data, under certain circumstances, Akamai Ghost erroneously forwards the invalid request and subsequent superfluous bytes to the origin server. An attacker could hide a smuggled request in these superfluous bytes. Whether this is exploitable depends on the origin server's behavior and how it processes the invalid request it receives from Akamai Ghost.	4.8	More Details
CVE-2025-66270	The KDE Connect protocol 8 before 2025-11-28 does not correlate device IDs across two packets. This affects KDE Connect before 25.12 on desktop, KDE Connect before 0.5.4 on iOS, KDE Connect before 1.34.4 on Android, GSConnect before 68, and Valent before 1.0.0.alpha.49.	4.7	More Details
CVE-2025-14229	A security vulnerability has been detected in SourceCodester Inventory Management System 1.0. The affected element is an unknown function of the component SVC Report Export. Such manipulation leads to csv injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-13992	Side-channel information leakage in Navigation and Loading in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	4.7	More Details

CVE-2025-14012	A vulnerability was determined in JIZHICMS up to 2.5.5. The affected element is the function deleteAll/findAll/delete of the file /index.php/admins/Comment/deleteAll.html of the component Batch Delete Comments. Executing manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-14004	A security flaw has been discovered in dayrui XunRuiCMS up to 4.7.1. Affected is an unknown function of the file /admind45f74adbd95.php?c=email&m=add of the component Email Setting Handler. Performing manipulation results in server-side request forgery. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-32898	The KDE Connect verification-code protocol before 2025-04-18 uses only 8 characters and therefore allows brute-force attacks. This affects KDE Connect before 1.33.0 on Android, KDE Connect before 25.04 on desktop, KDE Connect before 0.5 on iOS, Valent before 1.0.0.alpha.47, and GSConnect before 59.	4.7	More Details
CVE-2025-67585	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in flexmls Flexmls® IDX flexmls-idx allows Phishing.This issue affects Flexmls® IDX: from n/a through <= 3.15.7.	4.7	More Details
CVE-2025-14093	A vulnerability was detected in Edimax BR-6478AC V3 1.0.15. Impacted is the function sub_416990 of the file /boafrm/formTracerouteDiagnosticRun. The manipulation of the argument host results in os command injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-14008	A flaw has been found in dayrui XunRuiCMS up to 4.7.1. This vulnerability affects unknown code of the file admin79f2ec220c7e.php?c=api&m=test_site_domain of the component Project Domain Change Test. This manipulation of the argument v causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-14116	A vulnerability was detected in xerrors Yuxi-Know up to 0.4.0. This vulnerability affects the function OtherEmbedding.aencode of the file /src/models/embed.py. Performing manipulation of the argument health_url results in server-side request forgery. The attack can be initiated remotely. The exploit is now public and may be used. The patch is named 0ff771dc1933d5a6b78f804115e78a7d8625c3f3. To fix this issue, it is recommended to deploy a patch. The vendor responded with a vulnerability confirmation and a list of security measures they have established already (e.g. disabled URL parsing, disabled URL upload mode, removed URL-to-markdown conversion).	4.7	More Details
CVE-2025-14219	A weakness has been identified in Campcodes Retro Basketball Shoes Online Store 1.0. The impacted element is an unknown function of the file /admin/admin_running.php. Executing manipulation of the argument product_image can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-14094	A flaw has been found in Edimax BR-6478AC V3 1.0.15. The affected element is the function sub_44CCE4 of the file /boafrm/formSysCmd. This manipulation of the argument sysCmd causes os command injection. 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.	4.7	More Details
CVE-2025-14090	A security flaw has been discovered in AMTT Hotel Broadband Operation System 1.0. This affects an unknown part of the file /manager/card/cardmake_down.php. Performing manipulation of the argument ID results in sql injection. 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-2025-14092	A security vulnerability has been detected in Edimax BR-6478AC V3 1.0.15. This issue affects the function sub_416898 of the file /boafrm/formDebugDiagnosticRun. The manipulation of the argument host leads to os command injection. The attack can be initiated 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-2025-14011	A vulnerability was found in JIZHICMS up to 2.5.5. Impacted is the function commentlist of the file /index.php/admins/Comment/addcomment.html of the component Add Display Name Field. Performing manipulation of the argument aid/tid results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-48614	In rebootWipeUserData of RecoverySystem.java, there is a possible way to factory reset the device while in DSU mode due to a missing permission check. This could lead to physical denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	4.6	More Details
CVE-2025-12832	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 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.	4.6	More Details
CVE-2025-65229	A stored cross-site scripting (XSS) vulnerability exists in the web interface of Lyrion Music Server <= 9.0.3. An authenticated user with access to Settings Player can save arbitrary HTML/JavaScript in the Player name field. That value is stored by the server and later rendered without proper output encoding on the Information (Player Info) tab, causing the script to execute in the context of any user viewing that page.	4.6	More Details
CVE-2025-64498	Tuleap is an Open Source Suite for management of software development and collaboration. Tuleap Community Edition versions below 17.0.99.1762444754 and Tuleap Enterprise Edition versions prior to 17.0-2, 16.13-7 and 16.12-10 allow attackers trick victims into changing tracker general settings. This issue is fixed in version Tuleap Community Edition version 17.0.99.1762444754 and Tuleap Enterprise Edition versions 17.0-2, 16.13-7 and 16.12-10.	4.6	More Details
CVE-2025-64499	Tuleap is a free and open source suite for management of software development and collaboration. Tuleap Community Editon versions prior to 17.0.99.1762456922 and Tuleap Enterprise Edition versions prior to 17.0-2, 16.13-7 and 16.12-10 are vulnerable to CSRF attacks through planning management API. Attackers have access to create, edit or remove plans. This issue is fixed in Tuleap Community Edition version 17.0.99.1762456922 and Tuleap Enterprise Edtion versions 17.0-2, 16.13-7 and 16.12-10.	4.6	More Details
CVE-2025-64760	Tuleap is a free and open source suite for management of software development and collaboration. Versions of Tuleap Community Edition prior to 17.0.99.1763126988 and Tuleap Enterprise Edition prior to 17.0-3 and 16.13-8 have missing CSRF protections which allow attackers to create or remove tracker triggers. This issue is fixed in Tuleap Community Edition version 17.0.99.1763126988 and Tuleap Enterprise Edition versions 17.0-3 and 16.13-8.	4.6	More Details
CVE-2025-	Tuleap is a free and open source suite for management of software development and collaboration. Versions of Tuleap Community Edition prior to 17.0.99.1763803709 and Tuleap Enterprise Edition versions prior to 17.0-4 and 16.13-9 are mission CSRF protections in its tracker	4.6	More

65962	field dependencies, allowing attackers to modify tracker fields. This issue is fixed in Tuleap Community Edition version 17.0.99.1763803709 and Tuleap Enterprise Edition versions 17.0-4 and 16.13-9.		Details
CVE-2025-40939	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected device contains a USB port which allows unauthenticated connections. This could allow an attacker with physical access to the device to trigger reboot that could cause denial of service condition.	4.6	More Details
CVE-2025-41696	An attacker can use an undocumented UART port on the PCB as a side-channel with the user hardcoded credentials obtained from CVE-2025-41692 to gain read access to parts of the filesystem of the device.	4.6	More Details
CVE-2025-66510	Nextcloud Server is a self hosted personal cloud system. In Nextcloud Server prior to 31.0.10 and 32.0.1 and Nextcloud Enterprise Server prior to 28.0.14.11, 29.0.16.8, 30.0.17.3, and 31.0.10, contacts search allowed to retrieve personal data of other users (emails, names, identifiers) without proper access control. This allows an authenticated user to retrieve information about accounts that are not related or added as contacts.	4.5	More Details
CVE-2025-67467	Cross-Site Request Forgery (CSRF) vulnerability in StellarWP GiveWP give allows Cross Site Request Forgery.This issue affects GiveWP: from n/a through <= 4.13.1.	4.5	More Details
CVE-2025-12124	The FitVids for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12186	The Weekly Planner plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-13682	The Trail Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-58279	Permission control vulnerability in the media library module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.4	More Details
CVE-2025-63058	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Hiroaki Miyashita Custom Field Template custom-field-template allows Retrieve Embedded Sensitive Data.This issue affects Custom Field Template: from n/a through <= 2.7.4.	4.4	More Details
CVE-2025-62468	Out-of-bounds read in Windows Defender Firewall Service allows an authorized attacker to disclose information locally.	4.4	More Details
CVE-2025-20389	In Splunk Enterprise versions below 10.0.2, 9.4.6, 9.3.8, and 9.2.10, and versions below 3.9.10, 3.8.58 and 3.7.28 of the Splunk Secure Gateway app on Splunk Cloud Platform, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a malicious payload through the `label` column field after adding a new device in the Splunk Secure Gateway app. This could potentially lead to a client-side denial of service (DoS).	4.3	More Details
CVE-2025-20383	In Splunk Enterprise versions below 10.0.2, 9.4.6, 9.3.8, and 9.2.10, and below 3.9.10, 3.8.58, and 3.7.28 of Splunk Secure Gateway app in Splunk Cloud Platform, a low-privileged user that does not hold the "admin" or "power" Splunk roles and subscribes to mobile push notifications could receive notifications that disclose the title and description of the report or alert even if they do not have access to view the report or alert.	4.3	More Details
CVE-2025-67596	Cross-Site Request Forgery (CSRF) vulnerability in Strategy11 Team Business Directory business-directory-plugin allows Cross Site Request Forgery.This issue affects Business Directory: from n/a through <= 6.4.19.	4.3	More Details
CVE-2025-67595	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Quiz Maker quiz-maker allows Cross Site Request Forgery.This issue affects Quiz Maker: from n/a through <= 6.7.0.82.	4.3	More Details
CVE-2025-67594	Authorization Bypass Through User-Controlled Key vulnerability in ThimPress Thim Elementor Kit thim-elementor-kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Thim Elementor Kit: from n/a through <= 1.3.3.	4.3	More Details
CVE-2025-10055	The Time Sheets plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.3. This is due to missing or incorrect nonce validation on several endpoints. This makes it possible for unauthenticated attackers to perform a variety of actions 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-2025-12358	The ShopEngine Elementor WooCommerce Builder Addon plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.8.5. This is due to missing nonce validation on the "post_add_to_list" function as well as an incorrect permissions callback in the "Api/init" function. This makes it possible for unauthenticated attackers to add or remove products from a user's wishlist via a forged request granted they can trick a site's user into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-32899	In KDE Connect before 1.33.0 on Android, a packet can be crafted that causes two paired devices to unpair. Specifically, it is an invalid discovery packet sent over broadcast UDP.	4.3	More Details
CVE-2025-12782	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.9.4. This is due to the plugin not properly verifying a user's authorization in the disable() function. This makes it possible for authenticated attackers, with contributor level access and above, to disable the Beaver Builder layout on arbitrary posts and pages, causing content integrity issues and layout disruption on those pages.	4.3	More Details
	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all		

CVE-2025-13109	versions up to, and including, 1.3.7.2 via the "woof_add_query" and "woof_remove_query" functions due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber level access and above, to insert or remove arbitrary saved search queries into any user's profile, including administrators.	4.3	More Details
CVE-2025-13354	The Tag, Category, and Taxonomy Manager – AI Autotagger with OpenAI plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.40.1. This is due to the plugin not properly verifying that a user is authorized to perform an action in the "taxopress_merge_terms_batch" function. This makes it possible for authenticated attackers, with subscriber level access and above, to merge or delete arbitrary taxonomy terms.	4.3	More Details
CVE-2025-13362	The Norby AI plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.3. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update the plugin's 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.	4.3	More Details
CVE-2025-13756	The Fluent Booking plugin for WordPress is vulnerable to unauthorized calendar import and management due to a missing capability check on the "importCalendar" function in all versions up to, and including, 1.9.11. This makes it possible for authenticated attackers, with subscriber level access and above, to import arbitrary calendars and manage them.	4.3	More Details
CVE-2025-67598	Cross-Site Request Forgery (CSRF) vulnerability in PSM Plugins SupportCandy supportcandy allows Cross Site Request Forgery.This issue affects SupportCandy: from n/a through <= 3.4.1.	4.3	More Details
CVE-2025-14117	A vulnerability has been found in fit2cloud Halo 2.21.10. Impacted is an unknown function. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-22675	Cross-Site Request Forgery (CSRF) vulnerability in Taylor Hawkes WP Fast Cache allows Cross Site Request Forgery.This issue affects WP Fast Cache: from n/a through 1.5.	4.3	More Details
CVE-2025-67597	Missing Authorization vulnerability in Shahjahan Jewel Fluent Booking fluent-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent Booking: from n/a through <= 1.9.11.	4.3	More Details
CVE-2025-40819	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP4). Affected applications do not properly validate license restrictions against the database, allowing direct modification of the system_ticketinfo table to bypass license limitations without proper enforcement checks. This could allow with database access to circumvent licensing restrictions by directly modifying database values and potentially enabling unauthorized use beyond the permitted scope.	4.3	More Details
CVE-2025-67599	Missing Authorization vulnerability in WebToffee WebToffee eCommerce Marketing Automation decorator-woocommerce-email-customizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WebToffee eCommerce Marketing Automation: from n/a through <= 2.1.1.	4.3	More Details
CVE-2025-63077	Missing Authorization vulnerability in HappyMonster Happy Addons for Elementor happy-elementor-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Happy Addons for Elementor: from n/a through <= 3.20.2.	4.3	More Details
CVE-2025-33111	IBM Controller 11.1.0 through 11.1.1 and IBM Cognos Controller 11.0.0 through 11.0.1 FP6 is vulnerable to creation of temporary files without atomic operations which may expose sensitive information to an authenticated user due to race condition attacks.	4.3	More Details
CVE-2025-40941	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected devices exposes server information in its responses. This could allow an attacker with network access to gain useful information, increasing the likelihood of targeted attacks.	4.3	More Details
CVE-2025-66552	Nextcloud Server is a self hosted personal cloud system. In Nextcloud Server and Enterprise Server prior to 30.0.9 and 31.0.1, incorrect path handling with groupfolders caused the admin_audit app to not properly log all actions on files and folders inside groupfolders. This vulnerability is fixed in Nextcloud Server and Enterprise Server prior to 30.0.9 and 31.0.1.	4.3	More Details
CVE-2025-66547	Nextcloud Server is a self hosted personal cloud system. In Nextcloud Server and Enterprise Server prior to 31.0.1, non-privileged users can modify tags on files they should not have access to via bulk tagging. This vulnerability is fixed in 31.0.1.	4.3	More Details
CVE-2022-47425	Missing Authorization vulnerability in Repute Infosystems ARMember allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ARMember: from n/a through 3.4.10.	4.3	More Details
CVE-2025-67496	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Versions 3.5.4 and below contain a Stored Cross-Site Scripting (XSS) vulnerability in the /WeGIA/html/geral/configurar_senhas.php endpoint. The application does not sanitize user-controlled data before rendering it inside the employee selection dropdown. The application retrieves employee names from the database and injects them directly into HTML <option> elements without proper escaping. This issue is fixed in version 3.5.5.	4.3	More Details
CVE-2025-66553	Nextcloud Tables allows you to create your own tables with individual columns. Prior to 0.8.7 and 0.9.4, authenticated users were able to view meta data of columns in other tables of the Tables app by modifying the numeric ID in a request. This vulnerability is fixed in 0.8.7 and 0.9.4.	4.3	More Details
CVE-2025-14105	A vulnerability was determined in TOZED ZLT M30S and ZLT M30S PRO 1.47/3.09.06. This impacts an unknown function of the file /reqproc/proc_post of the component Web Interface. Executing manipulation of the argument goformId with the input REBOOT_DEVICE can lead to denial of service. The attack can only be done within the local network. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-41693	A low privileged remote attacker can use the ssh feature to execute commands directly after login. The process stays open and uses resources which leads to a reduced performance of the management functions. Switching functionality is not affected.	4.3	More Details
CVE-2025-65799	A lack of file name validation or verification in the Attachment service of usememos memos v0.25.2 allows attackers to execute a path traversal.	4.3	More Details

CVE-2025-63056	Missing Authorization vulnerability in bestwebsoft Contact Form by BestWebSoft contact-form-plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contact Form by BestWebSoft: from n/a through <= 4.3.5.	4.3	More Details
CVE-2025-62223	User interface (ui) misrepresentation of critical information in Microsoft Edge for iOS allows an unauthorized attacker to perform spoofing over a network.	4.3	More Details
CVE-2025-11759	The Backup, Restore and Migrate your sites with XCloner plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.8.2. This is due to missing or incorrect nonce validation on the Xcloner_Remote_Storage:save() function. This makes it possible for unauthenticated attackers to add or modify an FTP backup configuration via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Successful exploitation allows an attacker to set an attacker-controlled FTP site for backup storage and exfiltrate potentially sensitive site data.	4.3	More Details
CVE-2025-63060	Cross-Site Request Forgery (CSRF) vulnerability in hogash Kallyas kallyas.This issue affects Kallyas: from n/a through <= 4.2.	4.3	More Details
CVE-2025-12558	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.9.4 via the 'get_attachment_sizes' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including the path and meta data of private attachments, which can be used to view the attachments.	4.3	More Details
CVE-2025-63067	Missing Authorization vulnerability in p-themes Porto Theme - Functionality porto-functionality allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Porto Theme - Functionality: from n/a through <= 3.6.2.	4.3	More Details
CVE-2024-5401	Improper control of dynamically-managed code resources vulnerability in WebAPI component in Synology DiskStation Manager (DSM) before 7.1.1-42962-8 and 7.2.1-69057-2 and 7.2.2-72806 and Synology Unified Controller (DSMUC) before 3.1.4-23079 allows remote authenticated users to obtain privileges without consent via unspecified vectors.	4.3	More Details
CVE-2025-63070	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Shahjada Download Manager download-manager allows Retrieve Embedded Sensitive Data.This issue affects Download Manager: from n/a through <= 3.3.32.	4.3	More Details
CVE-2025-32901	In KDE Connect before 1.33.0 on Android, malicious device IDs (sent via broadcast UDP) could cause an application crash.	4.3	More Details
CVE-2025-13629	The WP Landing Page plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.9.3. This is due to missing nonce validation on the 'wplp_api_update_text' function. This makes it possible for unauthenticated attackers to update arbitrary post meta 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-2025-12574	The Listar – Directory Listing & Classifieds WordPress Plugin plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the '/wp-json/listar/v1/place/delete' REST API endpoint in all versions up to, and including, 3.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary posts.	4.3	More Details
CVE-2025-32900	In the KDE Connect information-exchange protocol before 2025-04-18, a packet can be crafted to temporarily change the displayed information about a device, because broadcast UDP is used. This affects KDE Connect before 1.33.0 on Android, KDE Connect before 25.04 on desktop, KDE Connect before 0.5 on iOS, Valent before 1.0.0.alpha.47, and GSConnect before 59.	4.3	More Details
CVE-2025-29844	A vulnerability in FileStation file cgi allows remote authenticated users to read file metadata and path information.	4.3	More Details
CVE-2025-14224	A vulnerability was found in Yottamaster DM2, DM3 and DM200 up to 1.2.23/1.9.12. Affected by this issue is some unknown functionality of the component File Upload. Performing manipulation results in path traversal. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-12128	The Hide Categories Or Products On Shop Page plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.7. This is due to missing or incorrect nonce validation on the save_data_hcps() function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-65796	Incorrect access control in usememos memos v0.25.2 allows attackers with low-level privileges to arbitrarily delete reactions made to other users' Memos.	4.3	More Details
CVE-2025-67593	Cross-Site Request Forgery (CSRF) vulnerability in Stiofan UsersWP userswp allows Cross Site Request Forgery.This issue affects UsersWP: from n/a through <= 1.2.48.	4.3	More Details
CVE-2025-12354	The Live CSS Preview plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_frontend_save' AJAX endpoint in all versions up to, and including, 2.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's css setting.	4.3	More Details
CVE-2025-12373	The Torod – The smart shipping and delivery portal for e-shops and retailers plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9. This is due to missing or incorrect nonce validation on the save_settings function. This makes it possible for unauthenticated attackers to modify plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-66513	Nextcloud Tables allows you to create your own tables with individual columns. Prior to 0.8.9, 0.9.6, and 1.0.1, the information which table (numeric ID) is shared with which groups or users and the respective permissions was not limited to privileged users. This vulnerability is fixed in 0.8.9, 0.9.6, and 1.0.1.	4.3	More Details
CVE-2025-67592	Missing Authorization vulnerability in Joe Dolson My Calendar my-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects My Calendar: from n/a through <= 3.6.16.	4.3	More Details

CVE-2025-67591	Cross-Site Request Forgery (CSRF) vulnerability in jegtheme JNews Paywall jnews-paywall allows Cross Site Request Forgery.This issue affects JNews Paywall: from n/a through < 12.0.1.	4.3	More Details
CVE-2025-67590	Cross-Site Request Forgery (CSRF) vulnerability in Rustaurius Ultimate FAQ ultimate-faqs allows Cross Site Request Forgery.This issue affects Ultimate FAQ: from n/a through <= 2.4.3.	4.3	More Details
CVE-2025-67589	Missing Authorization vulnerability in WP Overnight WooCommerce PDF Invoices & Packing Slips woocommerce-pdf-invoices-packing-slips allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce PDF Invoices & Packing Slips: from n/a through <= 4.9.1.	4.3	More Details
CVE-2025-13684	The ARK Related Posts plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 2.19. This is due to missing or incorrect nonce validation on the ark_rp_options_page function. This makes it possible for unauthenticated attackers to modify the plugin's configuration 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-2025-63012	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress WP Hotel Booking wp-hotel-booking allows Cross Site Request Forgery.This issue affects WP Hotel Booking: from n/a through <= 2.2.7.	4.3	More Details
CVE-2025-29845	A vulnerability in VideoPlayer2 subtitle cgi allows remote authenticated users to read .srt files.	4.3	More Details
CVE-2025-40935	A vulnerability has been identified in RUGGEDCOM RMC8388 V5.X (All versions < V5.10.1), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.10.1), RUGGEDCOM RS416v2 V5.X (All versions < V5.10.1), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.10.1), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.10.1), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.10.1), RUGGEDCOM RSG2100P (32M) V5.X (All versions < V5.10.1), RUGGEDCOM RSG2288 V5.X (All versions < V5.10.1), RUGGEDCOM RSG2300 V5.X (All versions < V5.10.1), RUGGEDCOM RSG2300P V5.X (All versions < V5.10.1), RUGGEDCOM RSG2488 V5.X (All versions < V5.10.1), RUGGEDCOM RSG907R (All versions < V5.10.1), RUGGEDCOM RSG908C (All versions < V5.10.1), RUGGEDCOM RSG909R (All versions < V5.10.1), RUGGEDCOM RSG910C (All versions < V5.10.1), RUGGEDCOM RSG920P V5.X (All versions < V5.10.1), RUGGEDCOM RSL910 (All versions < V5.10.1), RUGGEDCOM RST2228 (All versions < V5.10.1), RUGGEDCOM RST2228P (All versions < V5.10.1), RUGGEDCOM RST916C (All versions < V5.10.1), RUGGEDCOM RST916P (All versions < V5.10.1). Affected devices do not properly validate input during the TLS certificate upload process of the web service. This could allow an authenticated remote attacker to trigger a device crash and reboot, leading to a temporary Denial of Service on the device.	4.3	More Details
CVE-2025-12130	The WC Vendors – WooCommerce Multivendor, WooCommerce Marketplace, Product Vendors plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.4. This is due to missing or incorrect nonce validation on the /vendor_dashboard/product/delete/ endpoint. This makes it possible for unauthenticated attackers to delete vendor products 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-2025-13309	The Accessiy By CodeConfig Accessibility – Easy One-Click Accessibility Toolbar That Truly Matters plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 1.0.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers with subscriber-level access and above to modify the plugin’s global accessibility settings.	4.3	More Details
CVE-2025-12577	The Listar – Directory Listing & Classifieds WordPress Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the '/wp-json/listar/v1/place/save' REST API endpoint in all versions up to, and including, 3.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update listing details.	4.3	More Details
CVE-2025-14183	A vulnerability was found in SGAI Space1 NAS N1211DS up to 1.0.915. This issue affects the function GET_FACTORY_INFO/GET_USER_INFO of the file /cgi-bin/JSONAPI of the component gsaiagent. The manipulation results in unprotected storage of credentials. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-12091	The Search, Filters & Merchandising for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wcis_save_email' endpoint in all versions up to, and including, 3.0.63. This makes it possible for authenticated attackers, with Subscriber-level access and above, to deactivate the plugin.	4.3	More Details
CVE-2025-63681	open-webui v0.6.33 is vulnerable to Incorrect Access Control. The API /api/tasks/stop/ directly accesses and cancels tasks without verifying user ownership, enabling attackers (a normal user) to stop arbitrary LLM response tasks.	4.3	More Details
CVE-2025-13924	The Advanced Product Fields (Product Addons) for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6.17. This is due to missing or incorrect nonce validation on the 'maybe_duplicate' function. This makes it possible for unauthenticated attackers to duplicate and publish product field groups, including draft and pending field groups, 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-2025-36437	IBM Planning Analytics Local 2.1.0 - 2.1.15 could disclose sensitive information about server architecture that could aid in further attacks against the system.	4.3	More Details
CVE-2025-12133	The EPROLO Dropshipping plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wp_ajax_eprolo_delete_tracking and wp_ajax_eprolo_save_tracking_data AJAX endpoints in all versions up to, and including, 2.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify and delete tracking data.	4.3	More Details
CVE-2025-67587	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks WP Gravity Forms FreshDesk Plugin gf-freshdesk allows Phishing.This issue affects WP Gravity Forms FreshDesk Plugin: from n/a through <= 1.3.5.	4.3	More Details
CVE-2025-13360	The Quantic Social Image Hover plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.8. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update the plugin's 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.	4.3	More Details
CVE-2025-	The ContentStudio plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.7. This is due to missing or insufficient nonce validation on the add_cstu_settings function. This makes it possible for unauthenticated attackers to modify	4.3	More Details

13144	plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-12370	The Takeads plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.0.13. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete the plugin's configuration options.	4.3	More Details
CVE-2025-67588	Missing Authorization vulnerability in Elementor Elementor Website Builder elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Elementor Website Builder: from n/a through <= 3.33.0.	4.3	More Details
CVE-2025-12165	The Webcake – Landing Page Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'webcake_save_config' AJAX endpoint in all versions up to, and including, 1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's settings.	4.3	More Details
CVE-2025-12189	The Bread & Butter: Gate content + Capture leads + Collect first-party data + Nurture with Ai agents plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.10.1321. This is due to missing or incorrect nonce validation on the uploadImage() function. This makes it possible for unauthenticated attackers to upload arbitrary files that make remote code execution possible 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-2025-64056	File upload vulnerability in Fanvil x210 V2 2.12.20 allows unauthenticated attackers on the local network to store arbitrary files on the filesystem.	4.3	More Details
CVE-2025-14220	A security vulnerability has been detected in ORICO CD3510 1.9.12. This affects an unknown function of the component File Upload. The manipulation leads to path traversal. The attack can be initiated 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.	4.3	More Details
CVE-2025-12190	The Image Optimizer by wps.sk plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.0. This is due to missing or incorrect nonce validation on the imagopby_ajax_optimize_gallery() function. This makes it possible for unauthenticated attackers to trigger bulk optimization 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-2025-8148	An Improper Access Control in the SFTP service in Fortra's GoAnywhere MFT prior to version 7.9.0 allows Web Users with an Authentication Alias and a valid SSH key but limited to Password authentication for SFTP to still login using their SSH key.	4.2	More Details
CVE-2025-14345	A post-authentication flaw in the network two-phase commit protocol used for cross-shard transactions in MongoDB Server may lead to logical data inconsistencies under specific conditions which are not predictable and exist for a very short period of time. This error can cause the transaction coordination logic to misinterpret the transaction as committed, resulting in inconsistent state on those shards. This may lead to low integrity and availability impact. This issue impacts MongoDB Server v8.0 versions prior to 8.0.16, MongoDB Server v7.0 versions prior to 7.0.26 and MongoDB server v8.2 versions prior to 8.2.2.	4.2	More Details
CVE-2025-12996	Medtronic CareLink Network allows a local attacker with access to log files on an internal API server to view plaintext passwords from errors logged under certain circumstances. This issue affects CareLink Network: before December 4, 2025.	4.1	More Details
CVE-2025-66329	Permission control vulnerability in the window management module. Impact: Successful exploitation of this vulnerability may affect availability.	4.0	More Details
CVE-2025-64763	Envoy is a high-performance edge/middle/service proxy. In 1.33.12, 1.34.10, 1.35.6, 1.36.2, and earlier, when Envoy is configured in TCP proxy mode to handle CONNECT requests, it accepts client data before issuing a 2xx response and forwards that data to the upstream TCP connection. If a forwarding proxy upstream from Envoy then responds with a non-2xx status, this can cause a de-synchronized CONNECT tunnel state. By default Envoy continues to allow early CONNECT data to avoid disrupting existing deployments. The envoy.reloadable_features.reject_early_connect_data runtime flag can be set to reject CONNECT requests that send data before a 2xx response when intermediaries upstream from Envoy may reject establishment of a CONNECT tunnel.	3.7	More Details
CVE-2025-66629	HedgeDoc is an open source, real-time, collaborative, markdown notes application. Prior to 1.10.4, some of HedgeDoc's OAuth2 endpoints for social login providers such as Google, GitHub, GitLab, Facebook or Dropbox lack CSRF protection, since they don't send a state parameter and verify the response using this parameter. This vulnerability is fixed in 1.10.4.	3.7	More Details
CVE-2025-66514	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. Prior to 5.5.3, a stored HTML injection in the Mail app's message list allowed an authenticated user to inject HTML into the email subjects. Javascript was correctly blocked by the content security policy of the Nextcloud Server code.	3.5	More Details
CVE-2025-14221	A vulnerability was detected in SourceCodester Online Banking System 1.0. This impacts an unknown function of the file /?page=user. The manipulation of the argument First Name/Last Name results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2025-14186	A security flaw has been discovered in Grandstream GXP1625 1.0.7.4. The impacted element is an unknown function of the file /cgi-bin/api.values.post of the component Network Status Page. Performing manipulation of the argument vpn_ip results in basic cross site scripting. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-65228	A stored cross-site scripting vulnerability exists in the web management interface of the R.V.R. Elettronica TLK302T telemetry controller (firmware 1.5.1799).	3.5	More Details
CVE-2025-20382	In Splunk Enterprise versions below 10.0.2, 9.4.6, 9.3.8, and 9.2.10, and Splunk Cloud Platform versions below 10.1.2507.10, 10.0.2503.8, and 9.3.2411.120, a low-privileged user that does not hold the "admin" or "power" Splunk roles could create a views dashboard with a custom background using the `data:image/png;base64` protocol that could potentially lead to an unvalidated redirect. This behavior circumvents the Splunk external URL warning mechanism by using a specially crafted URL, allowing for a redirection to an external malicious site. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The authenticated user should not be able to exploit the vulnerability at will.	3.5	More Details
CVE-2025-63896	An issue in the Bluetooth Human Interface Device (HID) of JXL 9 Inch Car Android Double Din Player Android v12.0 allows attackers to inject arbitrary keystrokes via a spoofed Bluetooth HID device.	3.5	More Details

CVE-2025-14200	A vulnerability has been found in alokjaiswal Hotel-Management-services-using-MYSQL-and-php up to 5f8b60a7aa6c06a5632de569d4e3f6a8cd82f76f. Affected is an unknown function of the file /usersub.php of the component Request Pending Page. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-14194	A vulnerability was identified in code-projects Employee Profile Management System 1.0. This issue affects some unknown processing of the file /view_personnel.php. The manipulation of the argument per_address/dr_school/other_school leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2025-14228	A weakness has been identified in Yealink SIP-T21P E2 52.84.0.15. Impacted is an unknown function of the component Local Directory Page. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2025-66556	Nextcloud talk is a video & audio conferencing app for Nextcloud. Prior to 20.1.8 and 21.1.2, a participant with chat permissions was able to delete poll drafts of other participants within the conversation based on their numeric ID. This vulnerability is fixed in 20.1.8 and 21.1.2.	3.5	More Details
CVE-2025-66554	Contacts app for Nextcloud easily syncs contacts from various devices with your Nextcloud and allows editing. Prior to 5.5.4, 6.0.6, and 7.2.5, a malicious user was able to modify their organisation and title field to load additional CSS files. Javascript and other options were correctly blocked by the content security policy of the Nextcloud Server code. This vulnerability is fixed in 5.5.4, 6.0.6, and 7.2.5.	3.5	More Details
CVE-2025-66545	Nextcloud Groupfolders provides admin-configured folders shared by everyone in a group or team. Prior to 14.0.11, 15.3.12, 16.0.15, 17.0.14, 18.1.8, 19.1.8, and 20.1.2, a user with read-only permission can restore a file from the trash bin. This vulnerability is fixed in 14.0.11, 15.3.12, 16.0.15, 17.0.14, 18.1.8, 19.1.8, and 20.1.2.	3.5	More Details
CVE-2025-14006	A security vulnerability has been detected in dayrui XunRuiCMS up to 4.7.1. Affected by this issue is some unknown functionality of the file /admind45f74adbd95.php?c=field&m=add&rname=site&rid=1&page=1 of the component Add Data Validation Page. The manipulation of the argument data[name] leads to cross site scripting. 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.	3.5	More Details
CVE-2025-66333	Denial of service (DoS) vulnerability in the office service. Impact: Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-66546	Nextcloud Calendar is a calendar app for Nextcloud. Prior to 4.7.19, 5.5.6, and 6.0.1, the calendar app allowed blindly booking appointments with a squential ID without known the appointment token. This vulnerability is fixed in 4.7.19, 5.5.6, and 6.0.1.	3.3	More Details
CVE-2025-66548	Nextcloud Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. Prior to 1.12.7, 1.14.4, and 1.15.1, file extension can be spoofed by using RTLO characters, tricking users into download files with a different extension than what is displayed. This vulnerability is fixed in 1.12.7, 1.14.4, and 1.15.1.	3.3	More Details
CVE-2025-64786	Acrobat Reader versions 24.001.30264, 20.005.30793, 25.001.20982, 24.001.30273, 20.005.30803 and earlier are affected by an Improper Verification of Cryptographic Signature vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to gain limited unauthorized write access. Exploitation of this issue does not require user interaction.	3.3	More Details
CVE-2025-66334	Denial of service (DoS) vulnerability in the office service. Impact: Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-40818	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP4). Affected applications contain private SSL/TLS keys on the server that are not properly protected allowing any user with server access to read these keys. This could allow an authenticated attacker to impersonate the server potentially enabling man-in-the-middle, traffic decryption or unauthorized access to services that trust these certificates.	3.3	More Details
CVE-2025-60912	phpIPAM v1.7.3 contains a Cross-Site Request Forgery (CSRF) vulnerability in the database export functionality. The generate-mysql.php function, located in the /app/admin/import-export/ endpoint, allows remote attackers to trigger large database dump downloads via crafted HTTP GET requests if an administrator has an active session.	3.3	More Details
CVE-2025-66331	Denial of service (DoS) vulnerability in the office service. Impact: Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-66332	Denial of service (DoS) vulnerability in the office service. Impact: Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-64787	Acrobat Reader versions 24.001.30264, 20.005.30793, 25.001.20982, 24.001.30273, 20.005.30803 and earlier are affected by an Improper Verification of Cryptographic Signature vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass cryptographic protections and gain limited unauthorized write access. Exploitation of this issue does not require user interaction.	3.3	More Details
CVE-2025-66558	Nextcloud Twofactor WebAuthn is the WebAuthn Two-Factor Provider for Nextcloud. Prior to 1.4.2 and 2.4.1, a missing ownership check allowed an attack to take-away a 2FA webauthn device when correctly guessing a 80-128 character long random string of letters, numbers and symbols. The victim would then be prompted to register a new device on the next login. The attacker can not authenticate as the victim. This vulnerability is fixed in 1.4.2 and 2.4.1.	3.1	More Details
CVE-2025-12954	The Timetable and Event Schedule by MotoPress WordPress plugin before 2.4.16 does not verify a user has access to a specific event when duplicating, leading to arbitrary event disclosure when to users with a role as low as Contributor.	2.7	More Details
CVE-2024-56464	IBM QRadar SIEM 7.5 - 7.5.0 UP14 IF01 is affected by an information disclosure vulnerability involving exposure of directory information. IBM has addressed this vulnerability in the latest update.	2.7	More Details
CVE-	The Nextcloud Approval app allows approval or disapproval of files in the sidebar. Prior to 1.3.1 and 2.5.0, an authenticated user listed as a		

2025-66515	requester in a workflow can set another user's file into the "pending approval" without access to the file by using the numeric file id. This vulnerability is fixed in 1.3.1 and 2.5.0.	2.7	More Details
CVE-2025-20388	In Splunk Enterprise versions below 10.0.1, 9.4.6, 9.3.8, and 9.2.10, and Splunk Cloud Platform versions below 10.1.2507.4, 10.0.2503.7, and 9.3.2411.116, a user who holds a role that contains the high privilege capability `change_authentication` could enumerate internal IP addresses and network ports when adding new search peers to a Splunk search head in a distributed environment.	2.7	More Details
CVE-2025-57823	A direct request ('forced browsing') vulnerability in Fortinet FortiAuthenticator 6.6.0 through 6.6.6, FortiAuthenticator 6.5 all versions, FortiAuthenticator 6.4 all versions, FortiAuthenticator 6.3 all versions may allow an authenticated attacker with at least sponsor permissions to read and download device logs via accessing specific endpoints	2.7	More Details
CVE-2025-36102	IBM Controller 11.1.0 through 11.1.1 and IBM Cognos Controller 11.0.0 through 11.0.1 FP6 could allow a privileged user to bypass validation, passing user input into the application as trusted data, due to client-side enforcement of server-side security.	2.7	More Details
CVE-2025-59923	An improper access control vulnerability in Fortinet FortiAuthenticator 6.6.0 through 6.6.4, FortiAuthenticator 6.5 all versions, FortiAuthenticator 6.4 all versions, FortiAuthenticator 6.3 all versions may allow an authenticated attacker with at least read-only admin permission to obtain the credentials of other administrators' messaging services via crafted requests.	2.7	More Details
CVE-2025-20385	In Splunk Enterprise versions below 10.0.2, 9.4.6, 9.3.8, and 9.2.10, and Splunk Cloud Platform versions below 10.1.2507.6, 10.0.2503.7, and 9.3.2411.117, a user who holds a role with a high privilege capability `admin_all_objects` could craft a malicious payload through the href attribute of an anchor tag within a collection in the navigation bar, which could result in execution of unauthorized JavaScript code in the browser of a user.	2.4	More Details
CVE-2025-66549	Nextcloud Desktop is the desktop sync client for Nextcloud. Prior to 3.16.5, when trying to manually lock a file inside an end-to-end encrypted directory, the path of the file was sent to the server unencrypted, making it possible for administrators to see it in log files. This vulnerability is fixed in 3.16.5.	2.4	More Details
CVE-2025-14244	A flaw has been found in GreenCMS 2.3.0603. Affected by this issue is some unknown functionality of the file /Admin/Controller/CustomController.class.php of the component Menu Management Page. This manipulation of the argument Link causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2.4	More Details
CVE-2025-14201	A vulnerability was found in alokjaiswal Hotel-Management-services-using-MYSQL-and-php up to 5f8b60a7aa6c06a5632de569d4e3f6a8cd82f76f. Affected by this vulnerability is an unknown functionality of the file /dishsub.php. The manipulation of the argument item.name results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-14205	A vulnerability was found in code-projects Chamber of Commerce Membership Management System 1.0. Impacted is an unknown function of the file /membership_profile.php of the component Your Info Handler. Performing manipulation of the argument Full Name/Address/City/State results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2.4	More Details
CVE-2025-14005	A weakness has been identified in dayrui XunRuiCMS up to 4.7.1. Affected by this vulnerability is an unknown functionality of the file /admind45f74adbd95.php?c=field&m=add&rname=site&rid=1&page=0 of the component Add Display Name Field. Executing manipulation of the argument data[name] can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-14013	A vulnerability was identified in JIZHICMS up to 2.5.5. The impacted element is an unknown function of the file /index.php/admins/Comment/addcomment.html of the component Comment Handler. The manipulation of the argument body leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-12997	Insecure Direct Object Reference vulnerability in Medtronic CareLink Network which allows an authenticated attacker with access to specific device and user information to submit web requests to an API endpoint that would expose sensitive user information. This issue affects CareLink Network: before December 4, 2025.	2.2	More Details
CVE-2025-14007	A vulnerability was detected in dayrui XunRuiCMS up to 4.7.1. This affects an unknown part of the file /admin79f2ec220c7e.php?c=api&m=demo&name=mobile of the component Domain Name Binding Page. The manipulation results in cross site scripting. The attack may be performed from remote. A high complexity level is associated with this attack. It is indicated that the exploitability is 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.	2.0	More Details
CVE-2025-40259	In the Linux kernel, the following vulnerability has been resolved: scsi: sg: Do not sleep in atomic context sg_finish_rem_req() calls blk_rq_unmap_user(). The latter function may sleep. Hence, call sg_finish_rem_req() with interrupts enabled instead of disabled.	N/A	More Details
CVE-2021-47705	COMMAX UMS Client ActiveX Control 1.7.0.2 contains a heap-based buffer overflow vulnerability that allows attackers to execute arbitrary code by providing excessively long string arrays through multiple functions. Attackers can exploit improper boundary validation in CNC_Ctrl.dll to cause heap corruption and potentially gain system-level access.	N/A	More Details
CVE-2021-47704	OpenBMCS 2.4 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting arbitrary SQL code. Attackers can send GET requests to /debug/obix_test.php with malicious 'id' values to extract database information.	N/A	More Details
CVE-2025-40256	In the Linux kernel, the following vulnerability has been resolved: xfrm: also call xfrm_state_delete_tunnel at destroy time for states that were never added In commit b441cf3f8c4b ("xfrm: delete x->tunnel as we delete x"), I missed the case where state creation fails between full initialization (->init_state has been called) and being inserted on the lists. In this situation, ->init_state has been called, so for IPcomp tunnels, the fallback tunnel has been created and added onto the lists, but the user state never gets added, because we fail before that. The user state doesn't go through __xfrm_state_delete, so we don't call xfrm_state_delete_tunnel for those states, and we end up leaking the FB tunnel. There are several codepaths affected by this: the add/update paths, in both net/key and xfrm, and the migrate code (xfrm_migrate, xfrm_state_migrate). A "proper" rollback of the init_state work would probably be doable in the add/update code, but for migrate it gets more complicated as multiple states may be involved. At some point, the new (not-inserted) state will be destroyed, so call xfrm_state_delete_tunnel during xfrm_state_gc_destroy. Most states will have their fallback tunnel cleaned up during __xfrm_state_delete, which solves the issue that b441cf3f8c4b (and other patches before it) aimed at. All states (including FB tunnels) will be removed from the lists once xfrm_state_fini has called flush_work(&xfrm_state_gc_work).	N/A	More Details

CVE-2025-40255	In the Linux kernel, the following vulnerability has been resolved: net: core: prevent NULL deref in generic_hwtstamp_ioctl_lower() The ethtool tsconfig Netlink path can trigger a null pointer dereference. A call chain such as: tsconfig_prepare_data() -> dev_get_hwtstamp_phylib() -> vlan_hwtstamp_get() -> generic_hwtstamp_get_lower() -> generic_hwtstamp_ioctl_lower() results in generic_hwtstamp_ioctl_lower() being called with kernel_cfg->ifr as NULL. The generic_hwtstamp_ioctl_lower() function does not expect a NULL ifr and dereferences it, leading to a system crash. Fix this by adding a NULL check for kernel_cfg->ifr in generic_hwtstamp_ioctl_lower(). If ifr is NULL, return -EINVAL.	N/A	More Details
CVE-2025-40258	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix race condition in mptcp_schedule_work() syzbot reported use-after-free in mptcp_schedule_work() [1] Issue here is that mptcp_schedule_work() schedules a work, then gets a refcount on sk->sk_refcnt if the work was scheduled. This refcount will be released by mptcp_worker(). [A] if (schedule_work(...)) { [B] sock_hold(sk); return true; } Problem is that mptcp_worker() can run immediately and complete before [B] We need instead : sock_hold(sk); if (schedule_work(...)) return true; sock_put(sk); [1] refcount_t: addition on 0; use-after-free. WARNING: CPU: 1 PID: 29 at lib/refcount.c:25 refcount_warn_saturate+0xfa/0x1d0 lib/refcount.c:25 Call Trace: <TASK> __refcount_add include/linux/refcount.h:-1 [inline] __refcount_inc include/linux/refcount.h:366 [inline] refcount_inc include/linux/refcount.h:383 [inline] sock_hold include/net/sock.h:816 [inline] mptcp_schedule_work+0x164/0x1a0 net/mptcp/protocol.c:943 mptcp_tout_timer+0x21/0xa0 net/mptcp/protocol.c:2316 call_timer_fn+0x17e/0x5f0 kernel/time/timer.c:1747 expire_timers kernel/time/timer.c:1798 [inline] __run_timers kernel/time/timer.c:2372 [inline] __run_timer_base+0x648/0x970 kernel/time/timer.c:2384 run_timer_base kernel/time/timer.c:2393 [inline] run_timer_softirq+0xb7/0x180 kernel/time/timer.c:2403 handle_softirqs+0x22f/0x710 kernel/softirq.c:622 __do_softirq kernel/softirq.c:656 [inline] run_ktimerd+0xcf/0x190 kernel/softirq.c:1138 smpboot_thread_fn+0x542/0xa60 kernel/smpboot.c:160 kthread+0x711/0x8a0 kernel/kthread.c:463 ret_from_fork+0x4bc/0x870 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245	N/A	More Details
CVE-2021-47703	OpenBMCS 2.4 contains an unauthenticated SSRF vulnerability that allows attackers to bypass firewalls and initiate service and network enumeration on the internal network through the affected application, allowing hijacking of current sessions. Attackers can specify an external domain in the 'ip' parameter to force the application to make an HTTP request to an arbitrary destination host.	N/A	More Details
CVE-2025-40257	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix a race in mptcp_pm_del_add_timer() mptcp_pm_del_add_timer() can call sk_stop_timer_sync(sk, &entry->add_timer) while another might have free entry already, as reported by syzbot. Add RCU protection to fix this issue. Also change confusing add_timer variable with stop_timer boolean. syzbot report: BUG: KASAN: slab-use-after-free in __timer_delete_sync+0x372/0x3f0 kernel/time/timer.c:1616 Read of size 4 at addr ffff8880311e4150 by task kworker/1:1/44 CPU: 1 UID: 0 PID: 44 Comm: kworker/1:1 Not tainted syzkaller #0 PREEMPT_{RT,(full)} Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/02/2025 Workqueue: events mptcp_worker Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 __timer_delete_sync+0x372/0x3f0 kernel/time/timer.c:1616 sk_stop_timer_sync+0x1b/0x90 net/core/sock.c:3631 mptcp_pm_del_add_timer+0x283/0x310 net/mptcp/pm.c:362 mptcp_incoming_options+0x1357/0x1f60 net/mptcp/options.c:1174 tcp_data_queue+0xca/0x6450 net/ipv4/tcp_input.c:5361 tcp_rcv_established+0x1335/0x2670 net/ipv4/tcp_input.c:6441 tcp_v4_do_rcv+0x98b/0xbf0 net/ipv4/tcp_ipv4.c:1931 tcp_v4_rcv+0x252a/0x2dc0 net/ipv4/tcp_ipv4.c:2374 ip_protocol_deliver_rcu+0x221/0x440 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x3bb/0x6f0 net/ipv4/ip_input.c:239 NF_HOOK+0x30c/0x3a0 include/linux/netfilter.h:318 NF_HOOK+0x30c/0x3a0 include/linux/netfilter.h:318 __netif_receive_skb_one_core net/core/dev.c:6079 [inline] __netif_receive_skb+0x143/0x380 net/core/dev.c:6192 process_backlog+0x31e/0x900 net/core/dev.c:6544 __napi_poll+0xb6/0x540 net/core/dev.c:7594 napi_poll net/core/dev.c:7657 [inline] net_rx_action+0x5f7/0xda0 net/core/dev.c:7784 handle_softirqs+0x22f/0x710 kernel/softirq.c:622 __do_softirq kernel/softirq.c:656 [inline] __local_bh_enable_ip+0x1a0/0x2e0 kernel/softirq.c:302 mptcp_pm_send_ack net/mptcp/pm.c:210 [inline] mptcp_pm_addr_send_ack+0x41f/0x500 net/mptcp/pm.c:-1 mptcp_pm_worker+0x174/0x320 net/mptcp/pm.c:1002 mptcp_worker+0xd5/0x1170 net/mptcp/protocol.c:2762 process_one_work kernel/workqueue.c:3263 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3346 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3427 kthread+0x711/0x8a0 kernel/kthread.c:463 ret_from_fork+0x4bc/0x870 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> Allocated by task 44: kasan_save_stack mm/kasan/common.c:56 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:77 poison_kmalloc_redzone mm/kasan/common.c:400 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:417 kasan_kmalloc include/linux/kasan.h:262 [inline] __kmalloc_cache_noprof+0x1ef/0x6c0 mm/slub.c:5748 kmalloc_noprof include/linux/slab.h:957 [inline] mptcp_pm_alloc_anno_list+0x104/0x460 net/mptcp/pm.c:385 mptcp_pm_create_subflow_or_signal_addr+0xf9d/0x1360 net/mptcp/pm_kernel.c:355 mptcp_pm_nl_fully_established net/mptcp/pm_kernel.c:409 [inline] __mptcp_pm_kernel_worker+0x417/0x1ef0 net/mptcp/pm_kernel.c:1529 mptcp_pm_worker+0x1ee/0x320 net/mptcp/pm.c:1008 mptcp_worker+0xd5/0x1170 net/mptcp/protocol.c:2762 process_one_work kernel/workqueue.c:3263 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3346 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3427 kthread+0x711/0x8a0 kernel/kthread.c:463 ret_from_fork+0x4bc/0x870 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 Freed by task 6630: kasan_save_stack mm/kasan/common.c:56 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:77 __kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:587 kasan_save_free_info mm/kasan/kasan.h:406 [inline] poison_slab_object m --- truncated---	N/A	More Details
CVE-2025-40262	In the Linux kernel, the following vulnerability has been resolved: Input: imx_sc_key - fix memory corruption on unload This is supposed to be "priv" but we accidentally pass "&priv" which is an address in the stack and so it will lead to memory corruption when the imx_sc_key_action() function is called. Remove the &.	N/A	More Details
CVE-2025-40260	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix scx_enable() crash on helper kthread creation failure A crash was observed when the sched_ext selftests runner was terminated with Ctrl+\ while test 15 was running: NIP [c00000000028fa58] scx_enable.constprop.0+0x358/0x12b0 LR [c00000000028fa2c] scx_enable.constprop.0+0x32c/0x12b0 Call Trace: scx_enable.constprop.0+0x32c/0x12b0 (unreliable) bpf_struct_ops_link_create+0x18c/0x22c __sys_bpf+0x23f8/0x3044 sys_bpf+0x2c/0x6c system_call_exception+0x124/0x320 system_call_vectored_common+0x15c/0x2ec kthread_run_worker() returns an ERR_PTR() on failure rather than NULL, but the current code in scx_alloc_and_add_sched() only checks for a NULL helper. Incase of failure on SIGQUIT, the error is not handled in scx_alloc_and_add_sched() and scx_enable() ends up dereferencing an error pointer. Error handling is fixed in scx_alloc_and_add_sched() to propagate PTR_ERR() into ret, so that scx_enable() jumps to the existing error path, avoiding random dereference on failure.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nvme: nvme-fc: Ensure ->ioerr_work is cancelled in nvme_fc_delete_ctrl() nvme_fc_delete_assocation() waits for pending I/O to complete before returning, and an error can cause ->ioerr_work to be queued after cancel_work_sync() had been called. Move the call to cancel_work_sync() to be after nvme_fc_delete_association() to ensure ->ioerr_work is not running when the nvme_fc_ctrl object is freed. Otherwise the following can occur: [1135.911754] list_del corruption, ff2d24c8093f31f8->next is NULL [1135.917705] ------------[cut here]------------ [1135.922336] kernel BUG at lib/list_debug.c:52! [1135.926784] Oops: invalid opcode: 0000 [#1] SMP NOPTI [1135.931851] CPU: 48 UID: 0 PID: 726 Comm: kworker/u449:23 Kdump: loaded Not tainted 6.12.0 #1 PREEMPT(voluntary) [1135.943490] Hardware name: Dell Inc. PowerEdge R660/0HGTK9, BIOS 2.5.4 01/16/2025 [1135.950969] Workqueue: 0x0 (nvme-wq) [1135.954673] RIP: 0010:__list_del_entry_valid_or_report.cold+0xf/0x6f [1135.961041] Code: c7 c7 98 68 72 94 e8 26 45 fe ff 0f 0b 48 c7 c7 70 68 72 94 e8 18 45 fe ff 0f 0b 48 89 fe 48 c7 c7 80 69 72 94 e8 07 45 fe ff <0f> 0b 48 89 d1 48 c7 c7 a0 6a 72 94 48 89 c2 e8 f3 44 fe ff 0f 0b [1135.979788] RSP: 0018:ff579b19482d3e50 EFLAGS:		

CVE-2025-40261	00010046 [1135.985015] RAX: 0000000000000033 RBX: ff2d24c8093f31f0 RCX: 0000000000000000 [1135.992148] RDX: 0000000000000000 RSI: ff2d24d6bfa1d0c0 RDI: ff2d24d6bfa1d0c0 [1135.999278] RBP: ff2d24c8093f31f8 R08: 0000000000000000 R09: ffffffff951e2b08 [1136.006413] R10: ffffffff95122ac8 R11: 0000000000000003 R12: ff2d24c78697c100 [1136.013546] R13: fffffffffffffff8 R14: 0000000000000000 R15: ff2d24c78697c0c0 [1136.020677] FS: 0000000000000000(0000) GS:ff2d24d6bfa00000(0000) knlGS:0000000000000000 [1136.028765] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [1136.034510] CR2: 00007fd207f90b80 CR3: 000000163ea22003 CR4: 0000000000f73ef0 [1136.041641] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [1136.048776] DR3: 0000000000000000 DR6: 00000000fffe07f0 DR7: 0000000000000400 [1136.055910] PKRU: 55555554 [1136.058623] Call Trace: [1136.061074] <TASK> [1136.063179] ? show_trace_log_lvl+0x1b0/0x2f0 [1136.067540] ? show_trace_log_lvl+0x1b0/0x2f0 [1136.071898] ? move_linked_works+0x4a/0xa0 [1136.075998] ? __list_del_entry_valid_or_report.cold+0xf/0x6f [1136.081744] ? __die_body.cold+0x8/0x12 [1136.085584] ? die+0x2e/0x50 [1136.088469] ? do_trap+0xca/0x110 [1136.091789] ? do_error_trap+0x65/0x80 [1136.095543] ? __list_del_entry_valid_or_report.cold+0xf/0x6f [1136.101289] ? exc_invalid_op+0x50/0x70 [1136.105127] ? __list_del_entry_valid_or_report.cold+0xf/0x6f [1136.110874] ? asm_exc_invalid_op+0x1a/0x20 [1136.115059] ? __list_del_entry_valid_or_report.cold+0xf/0x6f [1136.120806] move_linked_works+0x4a/0xa0 [1136.124733] worker_thread+0x216/0x3a0 [1136.128485] ? __pfx_worker_thread+0x10/0x10 [1136.132758] kthread+0xfa/0x240 [1136.135904] ? __pfx_kthread+0x10/0x10 [1136.139657] ret_from_fork+0x31/0x50 [1136.143236] ? __pfx_kthread+0x10/0x10 [1136.146988] ret_from_fork_asm+0x1a/0x30 [1136.150915] </TASK>	N/A	More Details
CVE-2021-47708	COMMAX Smart Home System CDP-1020n contains an SQL injection vulnerability that allows attackers to bypass authentication by injecting arbitrary SQL code through the 'id' parameter in 'loginstart.asp'. Attackers can exploit this by sending a POST request with malicious 'id' values to manipulate database queries and gain unauthorized access.	N/A	More Details
CVE-2025-63013	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in ThimPress WP Hotel Booking wp-hotel-booking allows Retrieve Embedded Sensitive Data.This issue affects WP Hotel Booking: from n/a through <= 2.2.7.	N/A	More Details
CVE-2025-63015	Missing Authorization vulnerability in paysera WooCommerce Payment Gateway – Paysera woo-payment-gateway-paysera allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Payment Gateway – Paysera: from n/a through <= 3.9.0.	N/A	More Details
CVE-2025-63023	Missing Authorization vulnerability in Easy Payment Payment Gateway for PayPal on WooCommerce woo-paypal-gateway allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Payment Gateway for PayPal on WooCommerce: from n/a through <= 9.0.52.	N/A	More Details
CVE-2025-63024	Missing Authorization vulnerability in tychesoftwares Order Delivery Date for WooCommerce order-delivery-date-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Order Delivery Date for WooCommerce: from n/a through <= 4.3.1.	N/A	More Details
CVE-2021-47707	COMMAX CVD-Axx DVR 5.1.4 contains weak default administrative credentials that allow remote password attacks and disclose RTSP stream. Attackers can exploit this by sending a POST request with the 'passkey' parameter set to '1234', allowing them to access the web control panel.	N/A	More Details
CVE-2025-63025	Missing Authorization vulnerability in Xagio SEO Xagio SEO xagio-seo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Xagio SEO: from n/a through <= 7.1.0.29.	N/A	More Details
CVE-2025-63028	Missing Authorization vulnerability in shinetheme Traveler traveler allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Traveler: from n/a through <= 3.2.6.	N/A	More Details
CVE-2021-47706	COMMAX Biometric Access Control System 1.0.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to access sensitive information and circumvent physical controls in smart homes and buildings by exploiting cookie poisoning. Attackers can forge cookies to bypass authentication and disclose sensitive information.	N/A	More Details
CVE-2025-63030	Cross-Site Request Forgery (CSRF) vulnerability in Saad Iqbal New User Approve new-user-approve allows Cross Site Request Forgery.This issue affects New User Approve: from n/a through <= 3.2.0.	N/A	More Details
CVE-2025-63033	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Riyadh Ahmed Make Section & Column Clickable For Elementor make-section-column-clickable-elementor allows Stored XSS.This issue affects Make Section & Column Clickable For Elementor: from n/a through <= 2.3.	N/A	More Details
CVE-2025-63034	Missing Authorization vulnerability in Steve Truman Page View Count page-views-count allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Page View Count: from n/a through <= 2.8.7.	N/A	More Details
CVE-2025-63035	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VibeThemes WPLMS wplms_plugin allows DOM-Based XSS.This issue affects WPLMS: from n/a through <= 1.9.9.5.4.	N/A	More Details
CVE-2025-63036	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in DFDevelopment Ronneby Theme Core ronneby-core allows PHP Local File Inclusion.This issue affects Ronneby Theme Core: from n/a through <= 1.5.68.	N/A	More Details
CVE-2021-47701	OpenBMCS 2.4 allows an attacker to escalate privileges from a read user to an admin user by manipulating permissions and exploiting a vulnerability in the update_user_permissions.php script. Attackers can submit a malicious HTTP POST request to PHP scripts in '/plugins/useradmin/' directory.	N/A	More Details
CVE-2021-47702	OpenBMCS 2.4 contains a CSRF vulnerability that allows attackers to perform actions with administrative privileges by exploiting the sendFeedback.php endpoint. Attackers can submit malicious requests to trigger unintended actions, such as sending emails or modifying system settings.	N/A	More Details
CVE-2025-65289	A stored Cross site scripting (XSS) vulnerability in the Mercury MR816v2 (081C3114 4.8.7 Build 110427 Rel 36550n) router allows a remote attacker on the LAN to inject JavaScript into the router's management UI by submitting a malicious hostname. The injected script is stored and later executed in the context of an administrator's browser (for example after DHCP release/renew triggers the interface to display the stored hostname). Because the management interface uses weak/basic authentication and does not properly protect or isolate session material, the XSS can be used to exfiltrate the admin session and perform administrative actions.	N/A	More Details

CVE-2025-40254	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: remove never-working support for setting nsh fields The validation of the set(nsh(...)) action is completely wrong. It runs through the nsh_key_put_from_nlattr() function that is the same function that validates NSH keys for the flow match and the push_nsh() action. However, the set(nsh(...)) has a very different memory layout. Nested attributes in there are doubled in size in case of the masked set(). That makes proper validation impossible. There is also confusion in the code between the 'masked' flag, that says that the nested attributes are doubled in size containing both the value and the mask, and the 'is_mask' that says that the value we're parsing is the mask. This is causing kernel crash on trying to write into mask part of the match with SW_FLOW_KEY_PUT() during validation, while validate_nsh() doesn't allocate any memory for it: BUG: kernel NULL pointer dereference, address: 0000000000000018 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 1c2383067 P4D 1c2383067 PUD 20b703067 PMD 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 8 UID: 0 Kdump: loaded Not tainted 6.17.0-rc4+ #107 PREEMPT(voluntary) RIP: 0010:nsh_key_put_from_nlattr+0x19d/0x610 [openvswitch] Call Trace: <TASK> validate_nsh+0x60/0x90 [openvswitch] validate_set.constprop.0+0x270/0x3c0 [openvswitch] __ovs_nla_copy_actions+0x477/0x860 [openvswitch] ovs_nla_copy_actions+0x8d/0x100 [openvswitch] ovs_packet_cmd_execute+0x1cc/0x310 [openvswitch] genl_family_rcv_msg_doit+0xdb/0x130 genl_family_rcv_msg+0x14b/0x220 genl_rcv_msg+0x47/0xa0 netlink_rcv_skb+0x53/0x100 genl_rcv+0x24/0x40 netlink_unicast+0x280/0x3b0 netlink_sendmsg+0x1f7/0x430 ___sys_sendmsg+0x36b/0x3a0 ___sys_sendmsg+0x87/0xd0 __sys_sendmsg+0x6d/0xd0 do_syscall_64+0x7b/0x2c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e The third issue with this process is that while trying to convert the non-masked set into masked one, validate_set() copies and doubles the size of the OVS_KEY_ATTR_NSH as if it didn't have any nested attributes. It should be copying each nested attribute and doubling them in size independently. And the process must be properly reversed during the conversion back from masked to a non-masked variant during the flow dump. In the end, the only two outcomes of trying to use this action are either validation failure or a kernel crash. And if somehow someone manages to install a flow with such an action, it will most definitely not do what it is supposed to, since all the keys and the masks are mixed up. Fixing all the issues is a complex task as it requires re-writing most of the validation code. Given that and the fact that this functionality never worked since introduction, let's just remove it altogether. It's better to re-introduce it later with a proper implementation instead of trying to fix it in stable releases.	N/A	More Details
CVE-2025-66457	Elysia is a Typescript framework for request validation, type inference, OpenAPI documentation and client-server communication. Versions 1.4.17 and below are subject to arbitrary code execution from cookie config. When dynamic cookies are enabled (e.g. there an existing cookie schema), the cookie config is injected into the compiled route without first being sanitised. Availability of this exploit is generally low, but when combined with GHSA-hxj9-33pp-j2cc, it allows for a full RCE chain. An attack requires write access to either the Elysia app's source code (in which case the vulnerability is meaningless) or write access to the cookie config (perhaps where it is assumed to be provisioned by the environment). This issue is fixed in version 1.4.18.	N/A	More Details
CVE-2025-64257	Missing Authorization vulnerability in Joe Dolson My Tickets my-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects My Tickets: from n/a through <= 2.1.0.	N/A	More Details
CVE-2025-64256	Cross-Site Request Forgery (CSRF) vulnerability in PressTigers Simple Folio simple-folio allows Cross Site Request Forgery.This issue affects Simple Folio: from n/a through <= 1.1.0.	N/A	More Details
CVE-2025-64255	Missing Authorization vulnerability in Bowo Admin and Site Enhancements (ASE) admin-site-enhancements allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Admin and Site Enhancements (ASE): from n/a through <= 8.0.8.	N/A	More Details
CVE-2025-64254	Missing Authorization vulnerability in Ronald Huereca Photo Block photo-block allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Photo Block: from n/a through <= 1.5.1.	N/A	More Details
CVE-2025-65573	Cross Site Request Forgery (CSRF) vulnerability in AllskyTeam AllSky v2024.12.06_06 allows remote attackers to cause a denial of service via function handle_interface_POST_and_status.	N/A	More Details
CVE-2025-40242	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix unlikely race in gdlm_put_lock In gdlm_put_lock(), there is a small window of time in which the DFL_UNMOUNT flag has been set but the lockspace hasn't been released, yet. In that window, dlm may still call gdlm_ast() and gdlm_bast(). To prevent it from dereferencing freed glock objects, only free the glock if the lockspace has actually been released.	N/A	More Details
CVE-2025-40243	In the Linux kernel, the following vulnerability has been resolved: hfs: fix KMSAN uninit-value issue in hfs_find_set_zero_bits() The syzbot reported issue in hfs_find_set_zero_bits(): == BUG: KMSAN: uninit-value in hfs_find_set_zero_bits+0x74d/0xb60 fs/hfs/bitmap.c:45 hfs_find_set_zero_bits+0x74d/0xb60 fs/hfs/bitmap.c:45 hfs_vbm_search_free+0x13c/0x5b0 fs/hfs/bitmap.c:151 hfs_extend_file+0x6a5/0x1b00 fs/hfs/extent.c:408 hfs_get_block+0x435/0x1150 fs/hfs/extent.c:353 __block_write_begin_int+0xa76/0x3030 fs/buffer.c:2151 block_write_begin fs/buffer.c:2262 [inline] cont_write_begin+0x10e1/0x1bc0 fs/buffer.c:2601 hfs_write_begin+0x85/0x130 fs/hfs/inode.c:52 cont_expand_zero fs/buffer.c:2528 [inline] cont_write_begin+0x35a/0x1bc0 fs/buffer.c:2591 hfs_write_begin+0x85/0x130 fs/hfs/inode.c:52 hfs_file_truncate+0x1d6/0xe60 fs/hfs/extent.c:494 hfs_inode_setattr+0x964/0xaa0 fs/hfs/inode.c:654 notify_change+0x1993/0x1aa0 fs/attr.c:552 do_truncate+0x28f/0x310 fs/open.c:68 do_ftruncate+0x698/0x730 fs/open.c:195 do_sys_ftruncate fs/open.c:210 [inline] __do_sys_ftruncate fs/open.c:215 [inline] __se_sys_ftruncate fs/open.c:213 [inline] __x64_sys_ftruncate+0x11b/0x250 fs/open.c:213 x64_sys_call+0xfe3/0x3db0 arch/x86/include/generated/asm/syscalls_64.h:78 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xd9/0x210 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:4154 [inline] slab_alloc_node mm/slub.c:4197 [inline] __kmalloc_cache_noprof+0x7f7/0xed0 mm/slub.c:4354 kmalloc_noprof include/linux/slab.h:905 [inline] hfs_mdb_get+0x1cc8/0x2a90 fs/hfs/mdb.c:175 hfs_fill_super+0x3d0/0xb80 fs/hfs/super.c:337 get_tree_bdev_flags+0x6e3/0x920 fs/super.c:1681 get_tree_bdev+0x38/0x50 fs/super.c:1704 hfs_get_tree+0x35/0x40 fs/hfs/super.c:388 vfs_get_tree+0xb0/0x5c0 fs/super.c:1804 do_new_mount+0x738/0x1610 fs/namespace.c:3902 path_mount+0x6db/0x1e90 fs/namespace.c:4226 do_mount fs/namespace.c:4239 [inline] __do_sys_mount fs/namespace.c:4450 [inline] __se_sys_mount+0x6eb/0x7d0 fs/namespace.c:4427 __x64_sys_mount+0xe4/0x150 fs/namespace.c:4427 x64_sys_call+0xfa7/0x3db0 arch/x86/include/generated/asm/syscalls_64.h:166 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xd9/0x210 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 1 UID: 0 PID: 12609 Comm: syz.1.2692 Not tainted 6.16.0-syzkaller #0 PREEMPT(none) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/12/2025 == The HFS_SB(sb)->bitmap buffer is allocated in hfs_mdb_get(): HFS_SB(sb)->bitmap = kmalloc(8192, GFP_KERNEL); Finally, it can trigger the reported issue because kmalloc() doesn't clear the allocated memory. If allocated memory contains only zeros, then everything will work pretty fine. But if the allocated memory contains the "garbage", then it can affect the bitmap operations and it triggers the reported issue. This patch simply exchanges the kmalloc() on kzalloc() with the goal to guarantee the correctness of bitmap operations. Because, newly created allocation bitmap should have all available blocks free. Potentially, initialization bitmap's read operation could not fill the whole allocated memory and "garbage" in the not initialized memory will be the reason of volume coruptions and file system driver bugs.	N/A	More Details

CVE-2025-40244	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix KMSAN uninit-value issue in __hfsplus_ext_cache_extent() The syzbot reported issue in __hfsplus_ext_cache_extent(): [70.194323][T9350] BUG: KMSAN: uninit-value in __hfsplus_ext_cache_extent+0x7d0/0x990 [70.195022][T9350] __hfsplus_ext_cache_extent+0x7d0/0x990 [70.195530][T9350] hfsplus_file_extend+0x74f/0x1cf0 [70.195998][T9350] hfsplus_get_block+0xe16/0x17b0 [70.196458][T9350] __block_write_begin_int+0x962/0x2ce0 [70.196959][T9350] cont_write_begin+0x1000/0x1950 [70.197416][T9350] hfsplus_write_begin+0x85/0x130 [70.197873][T9350] generic_perform_write+0x3e8/0x1060 [70.198374][T9350] __generic_file_write_iter+0x215/0x460 [70.198892][T9350] generic_file_write_iter+0x109/0x5e0 [70.199393][T9350] vfs_write+0xb0f/0x14e0 [70.199771][T9350] ksys_write+0x23e/0x490 [70.200149][T9350] __x64_sys_write+0x97/0xf0 [70.200570][T9350] x64_sys_call+0x3015/0x3cf0 [70.201065][T9350] do_syscall_64+0xd9/0x1d0 [70.201506][T9350] entry_SYSCALL_64_after_hwframe+0x77/0x7f [70.202054][T9350] [70.202279][T9350] Uninit was created at: [70.202693][T9350] __kmalloc_noprof+0x621/0xf80 [70.203149][T9350] hfsplus_find_init+0x8d/0x1d0 [70.203602][T9350] hfsplus_file_extend+0x6ca/0x1cf0 [70.204087][T9350] hfsplus_get_block+0xe16/0x17b0 [70.204561][T9350] __block_write_begin_int+0x962/0x2ce0 [70.205074][T9350] cont_write_begin+0x1000/0x1950 [70.205547][T9350] hfsplus_write_begin+0x85/0x130 [70.206017][T9350] generic_perform_write+0x3e8/0x1060 [70.206519][T9350] __generic_file_write_iter+0x215/0x460 [70.207042][T9350] generic_file_write_iter+0x109/0x5e0 [70.207552][T9350] vfs_write+0xb0f/0x14e0 [70.207961][T9350] ksys_write+0x23e/0x490 [70.208375][T9350] __x64_sys_write+0x97/0xf0 [70.208810][T9350] x64_sys_call+0x3015/0x3cf0 [70.209255][T9350] do_syscall_64+0xd9/0x1d0 [70.209680][T9350] entry_SYSCALL_64_after_hwframe+0x77/0x7f [70.210230][T9350] [70.210454][T9350] CPU: 2 UID: 0 PID: 9350 Comm: repro Not tainted 6.12.0-rc5 #5 [70.211174][T9350] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [70.212115][T9350] === [70.212734][T9350] Disabling lock debugging due to kernel taint [70.213284][T9350] Kernel panic - not syncing: kmsan.panic set ... [70.213858][T9350] CPU: 2 UID: 0 PID: 9350 Comm: repro Tainted: G B 6.12.0-rc5 #5 [70.214679][T9350] Tainted: [B]=BAD_PAGE [70.215057][T9350] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [70.215999][T9350] Call Trace: [70.216309][T9350] <TASK> [70.216585][T9350] dump_stack_lvl+0x1fd/0x2b0 [70.217025][T9350] dump_stack+0x1e/0x30 [70.217421][T9350] panic+0x502/0xca0 [70.217803][T9350] ? kmsan_get_metadata+0x13e/0x1c0 [70.218294][Message fromT sy9350] kmsan_report+0x296/slogd@syzkaller 0x2aat Aug 18 22:11:058 ... kernel :[70.213284][T9350] Kernel panic - not syncing: kmsan.panic [70.220179][T9350] ? kmsan_get_metadata+0x13e/0x1c0 set ... [70.221254][T9350] ? __msan_warning+0x96/0x120 [70.222066][T9350] ? __hfsplus_ext_cache_extent+0x7d0/0x990 [70.223023][T9350] ? hfsplus_file_extend+0x74f/0x1cf0 [70.224120][T9350] ? hfsplus_get_block+0xe16/0x17b0 [70.224946][T9350] ? __block_write_begin_int+0x962/0x2ce0 [70.225756][T9350] ? cont_write_begin+0x1000/0x1950 [70.226337][T9350] ? hfsplus_write_begin+0x85/0x130 [70.226852][T9350] ? generic_perform_write+0x3e8/0x1060 [70.227405][T9350] ? __generic_file_write_iter+0x215/0x460 [70.227979][T9350] ? generic_file_write_iter+0x109/0x5e0 [70.228540][T9350] ? vfs_write+0xb0f/0x14e0 [70.228997][T9350] ? ksys_write+0x23e/0x490 ---truncated---	N/A	More Details
CVE-2025-40245	In the Linux kernel, the following vulnerability has been resolved: nios2: ensure that memblock.current_limit is set when setting pfn limits On nios2, with CONFIG_FLATMEM set, the kernel relies on memblock_get_current_limit() to determine the limits of mem_map, in particular for max_low_pfn. Unfortunately, memblock.current_limit is only default initialized to MEMBLOCK_ALLOC_ANYWHERE at this point of the bootup, potentially leading to situations where max_low_pfn can erroneously exceed the value of max_pfn and, thus, the valid range of available DRAM. This can in turn cause kernel-level paging failures, e.g.: [76.900000] Unable to handle kernel paging request at virtual address 20303000 [76.900000] ea = c0080890, ra = c000462c, cause = 14 [76.900000] Kernel panic - not syncing: Oops [76.900000] ---[end Kernel panic - not syncing: Oops]--- This patch fixes this by pre-calculating memblock.current_limit based on the upper limits of the available memory ranges via adjust_lowmem_bounds, a simplified version of the equivalent implementation within the arm architecture.	N/A	More Details
CVE-2025-40246	In the Linux kernel, the following vulnerability has been resolved: xfs: fix out of bounds memory read error in symlink repair xfs/286 produced this report on my test fleet: == BUG: KFENCE: out-of-bounds read in memcpy_orig+0x54/0x110 Out-of-bounds read at 0xffff88843fe9e038 (184B right of kfence-#184): memcpy_orig+0x54/0x110 xrep_symlink_salvage_inline+0xb3/0xf0 [xfs] xrep_symlink_salvage+0x100/0x110 [xfs] xrep_symlink+0x2e/0x80 [xfs] xrep_attempt+0x61/0x1f0 [xfs] xfs_scrub_metadata+0x34f/0x5c0 [xfs] xfs_ioc_scrubv_metadata+0x387/0x560 [xfs] xfs_file_ioctl+0xe23/0x10e0 [xfs] __x64_sys_ioctl+0x76/0xc0 do_syscall_64+0x4e/0x1e0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 kfence-#184: 0xffff88843fe9df80-0xffff88843fe9dfea, size=107, cache=kmalloc-128 allocated by task 3470 on cpu 1 at 263329.131592s (192823.508886s ago): xfs_init_local_fork+0x79/0xe0 [xfs] xfs_iformat_local+0xa4/0x170 [xfs] xfs_iformat_data_fork+0x148/0x180 [xfs] xfs_inode_from_disk+0x2cd/0x480 [xfs] xfs_iget+0x450/0xd60 [xfs] xfs_bulkstat_one_int+0x6b/0x510 [xfs] xfs_bulkstat_iwalk+0x1e/0x30 [xfs] xfs_iwalk_ag_recs+0xdf/0x150 [xfs] xfs_iwalk_run_callbacks+0xb9/0x190 [xfs] xfs_iwalk_ag+0x1dc/0x2f0 [xfs] xfs_iwalk_args.constprop.0+0x6a/0x120 [xfs] xfs_iwalk+0xa4/0xd0 [xfs] xfs_bulkstat+0xfa/0x170 [xfs] xfs_ioc_fsbulkstat.isra.0+0x13a/0x230 [xfs] xfs_file_ioctl+0xbf2/0x10e0 [xfs] __x64_sys_ioctl+0x76/0xc0 do_syscall_64+0x4e/0x1e0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 CPU: 1 UID: 0 PID: 1300113 Comm: xfs_scrub Not tainted 6.18.0-rc4-djwx #rc4 PREEMPT(lazy) 3d744dd94e92690f00a04398d2bd8631dcef1954 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.0-4.module+el8.8.0+21164+ed375313 04/01/2014 == On further analysis, I realized that the second parameter to min() is not correct. xfs_ifork::if_bytes is the size of the xfs_ifork::if_data buffer. if_bytes can be smaller than the data fork size because: (a) the forkoff code tries to keep the data area as large as possible (b) for symbolic links, if_bytes is the ondisk file size + 1 (c) forkoff is always a multiple of 8. Case in point: for a single-byte symlink target, forkoff will be 8 but the buffer will only be 2 bytes long. In other words, the logic here is wrong and we walk off the end of the incore buffer. Fix that.	N/A	More Details
CVE-2025-65882	An issue was discovered in openmptcprouter thru 0.64 in file common/package/utils/sys-upgrade-helper/src/tools/sysupgrade.c in function create_xor_ipad_opad allowing attackers to potentially write arbitrary files or execute arbitrary commands.	N/A	More Details
CVE-2025-9612	An issue was discovered in the PCI Express (PCIe) Integrity and Data Encryption (IDE) specification, where insufficient guidance on Transaction Layer Packet (TLP) ordering and tag uniqueness may allow encrypted packets to be replayed or reordered without detection. This can enable local or physical attackers on the PCIe bus to violate data integrity protections.	N/A	More Details
CVE-2025-9613	A vulnerability was discovered in the PCI Express (PCIe) Integrity and Data Encryption (IDE) specification, where insufficient guidance on tag reuse after completion timeouts may allow multiple outstanding Non-Posted Requests to share the same tag. This tag aliasing condition can result in completions being delivered to the wrong security context, potentially compromising data integrity and confidentiality.	N/A	More Details
CVE-2025-9614	An issue was discovered in the PCI Express (PCIe) Integrity and Data Encryption (IDE) specification, where insufficient guidance on re-keying and stream flushing during device rebinding may allow stale write transactions from a previous security context to be processed in a new one. This can lead to unintended data access across trusted domains, compromising confidentiality and integrity.	N/A	More Details
CVE-2025-29864	Protection Mechanism Failure vulnerability in ESTsoft ALZip on Windows allows SmartScreen bypass.This issue affects ALZip: from 12.01 before 12.29.	N/A	More Details

CVE-2025-40247	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix pgtable prealloc error path The following splat was reported: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000010 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=00000008d0fd8000 [0000000000000010] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP CPU: 5 UID: 1000 PID: 149076 Comm: Xwayland Tainted: G S 6.16.0-rc2-00809-g0b6974bb4134-dirty #367 PREEMPT Tainted: [S]=CPU_OUT_OF_SPEC Hardware name: Qualcomm Technologies, Inc. SM8650 HDK (DT) pstate: 83400005 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : build_detached_freelist+0x28/0x224 lr : kmem_cache_free_bulk.part.0+0x38/0x244 sp : ffff000a508c7a20 x29: ffff000a508c7a20 x28: ffff000a508c7d50 x27: ffffc4e49d16f350 x26: 0000000000000058 x25: 00000000ffffffc x24: 0000000000000000 x23: ffff00098c4e1450 x22: 00000000ffffffc x21: 0000000000000000 x20: ffff000a508c7af8 x19: 0000000000000002 x18: 00000000000003e8 x17: ffff000809523850 x16: ffff000809523820 x15: 0000000000401640 x14: ffff000809371140 x13: 0000000000000130 x12: ffff0008b5711e30 x11: 00000000001058fa x10: 0000000000000a80 x9 : ffff000a508c7940 x8 : ffff000809371ba0 x7 : 781fffe033087fff x6 : 0000000000000000 x5 : ffff0008003cd000 x4 : 781fffe033083fff x3 : ffff000a508c7af8 x2 : fffffdffc0000000 x1 : 0001000000000000 x0 : ffff0008001a6a00 Call trace: build_detached_freelist+0x28/0x224 (P) kmem_cache_free_bulk.part.0+0x38/0x244 kmem_cache_free_bulk+0x10/0x1c msm_iommu_pagetable_prealloc_cleanup+0x3c/0xd0 msm_vma_job_free+0x30/0x240 msm_ioctl_vm_bind+0x1d0/0x9a0 drm_ioctl_kernel+0x84/0x104 drm_ioctl+0x358/0x4d4 __arm64_sys_ioctl+0x8c/0xe0 invoke_syscall+0x44/0x100 el0_svc_common.constprop.0+0x3c/0xe0 do_el0_svc+0x18/0x20 el0_svc+0x30/0x100 el0t_64_sync_handler+0x104/0x130 el0t_64_sync+0x170/0x174 Code: aa0203f5 b26287e2 f2dfbfe2 aa0303f4 (f8737ab6) ---[end trace 0000000000000000]--- Since msm_vma_job_free() is called directly from the ioctl, this looks like an error path cleanup issue. Which I think results from prealloc_cleanup() called without a preceding successful prealloc_allocate() call. So handle that case better. Patchwork: https://patchwork.freedesktop.org/patch/678677/	N/A	More Details
CVE-2025-64113	Emby Server is a user-installable home media server. Versions below 4.9.1.81 allow an attacker to gain full administrative access to an Emby Server (for Emby Server administration, not at the OS level). Other than network access, no specific preconditions need to be fulfilled for a server to be vulnerable. This issue is fixed in version 4.9.1.81.	N/A	More Details
CVE-2025-65741	Sublime Text 3 Build 3208 or prior for MacOS is vulnerable to Dylib Injection. An attacker could compile a .dylib file and force the execution of this library in the context of the Sublime Text application.	N/A	More Details
CVE-2025-13472	A fix was made in BlazeMeter Jenkins Plugin version 4.27 to allow users only with certain permissions to see the list of available resources like credential IDs, bzm workspaces and bzm project Ids. Prior to this fix, anyone could see this list as a dropdown on the Jenkins UI.	N/A	More Details
CVE-2025-40248	In the Linux kernel, the following vulnerability has been resolved: vsock: Ignore signal/timeout on connect() if already established During connect(), acting on a signal/timeout by disconnecting an already established socket leads to several issues: 1. connect() invoking vsock_transport_cancel_pkt() -> virtio_transport_purge_skbs() may race with sendmsg() invoking virtio_transport_get_credit(). This results in a permanently elevated `vvs->bytes_unsent`. Which, in turn, confuses the SOCK_LINGER handling. 2. connect() resetting a connected socket's state may race with socket being placed in a sockmap. A disconnected socket remaining in a sockmap breaks sockmap's assumptions. And gives rise to WARNs. 3. connect() transitioning SS_CONNECTED -> SS_UNCONNECTED allows for a transport change/drop after TCP_ESTABLISHED. Which poses a problem for any simultaneous sendmsg() or connect() and may result in a use-after-free/null-ptr-deref. Do not disconnect socket on signal/timeout. Keep the logic for unconnected sockets: they don't linger, can't be placed in a sockmap, are rejected by sendmsg(). [1]: https://lore.kernel.org/netdev/e07fd95c-9a38-4eea-9638-133e38c2ec9b@rbox.co/ [2]: https://lore.kernel.org/netdev/20250317-vsock-trans-signal-race-v4-0-fc8837f3f1d4@rbox.co/ [3]: https://lore.kernel.org/netdev/60f1b7db-3099-4f6a-875e-af9f6ef194f6@rbox.co/	N/A	More Details
CVE-2025-40249	In the Linux kernel, the following vulnerability has been resolved: gpio: cdev: make sure the cdev fd is still active before emitting events With the final call to fput() on a file descriptor, the release action may be deferred and scheduled on a work queue. The reference count of that descriptor is still zero and it must not be used. It's possible that a GPIO change, we want to notify the user-space about, happens AFTER the reference count on the file descriptor associated with the character device went down to zero but BEFORE the .release() callback was called from the workqueue and so BEFORE we unregistered from the notifier. Using the regular get_file() routine in this situation triggers the following warning: struct file::f_count incremented from zero; use-after-free condition present! So use the get_file_active() variant that will return NULL on file descriptors that have been or are being released.	N/A	More Details
CVE-2025-40250	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Clean up only new IRQ glue on request_irq() failure The mlx5_irq_alloc() function can inadvertently free the entire rmap and end up in a crash[1] when the other threads tries to access this, when request_irq() fails due to exhausted IRQ vectors. This commit modifies the cleanup to remove only the specific IRQ mapping that was just added. This prevents removal of other valid mappings and ensures precise cleanup of the failed IRQ allocation's associated glue object. Note: This error is observed when both fwctl and rds configs are enabled. [1] mlx5_core 0000:05:00.0: Successfully registered panic handler for port 1 mlx5_core 0000:05:00.0: mlx5_irq_alloc:293:(pid 66740): Failed to request irq. err = -28 infiniband mlx5_0: mlx5_ib_test_wc:290:(pid 66740): Error -28 while trying to test write-combining support mlx5_core 0000:05:00.0: Successfully unregistered panic handler for port 1 mlx5_core 0000:06:00.0: Successfully registered panic handler for port 1 mlx5_core 0000:06:00.0: mlx5_irq_alloc:293:(pid 66740): Failed to request irq. err = -28 infiniband mlx5_0: mlx5_ib_test_wc:290:(pid 66740): Error -28 while trying to test write-combining support mlx5_core 0000:06:00.0: Successfully unregistered panic handler for port 1 mlx5_core 0000:03:00.0: mlx5_irq_alloc:293:(pid 28895): Failed to request irq. err = -28 mlx5_core 0000:05:00.0: mlx5_irq_alloc:293:(pid 28895): Failed to request irq. err = -28 general protection fault, probably for non-canonical address 0xe277a58fde16f291: 0000 [#1] SMP NOPTI RIP: 0010:free_irq_cpu_rmap+0x23/0x7d Call Trace: <TASK> ? show_trace_log_lvl+0x1d6/0x2f9 ? show_trace_log_lvl+0x1d6/0x2f9 ? mlx5_irq_alloc.cold+0x5d/0xf3 [mlx5_core] ? __die_body.cold+0x8/0xa ? die_addr+0x39/0x53 ? exc_general_protection+0x1c4/0x3e9 ? dev_vprintk_emit+0x5f/0x90 ? asm_exc_general_protection+0x22/0x27 ? free_irq_cpu_rmap+0x23/0x7d mlx5_irq_alloc.cold+0x5d/0xf3 [mlx5_core] irq_pool_request_vector+0x7d/0x90 [mlx5_core] mlx5_irq_request+0x2e/0xe0 [mlx5_core] mlx5_irq_request_vector+0xad/0xf7 [mlx5_core] comp_irq_request_pci+0x64/0xf0 [mlx5_core] create_comp_eq+0x71/0x385 [mlx5_core] ? mlx5e_open_xdpsq+0x11c/0x230 [mlx5_core] mlx5_comp_eqn_get+0x72/0x90 [mlx5_core] ? xas_load+0x8/0x91 mlx5_comp_irqn_get+0x40/0x90 [mlx5_core] mlx5e_open_channel+0x7d/0x3c7 [mlx5_core] mlx5e_open_channels+0xad/0x250 [mlx5_core] mlx5e_open_locked+0x3e/0x110 [mlx5_core] mlx5e_open+0x23/0x70 [mlx5_core] __dev_open+0xf1/0x1a5 __dev_change_flags+0x1e1/0x249 dev_change_flags+0x21/0x5c do_setlink+0x28b/0xcc4 ? __nla_parse+0x22/0x3d ? inet6_validate_link_af+0x6b/0x108 ? cpumask_next+0x1f/0x35 ? __snmp6_fill_stats64.constprop.0+0x66/0x107 ? __nla_validate_parse+0x48/0x1e6 __rtnl_newlink+0x5ff/0xa57 ? kmem_cache_alloc_trace+0x164/0x2ce rtnl_newlink+0x44/0x6e rtnetlink_rcv_msg+0x2bb/0x362 ? __netlink_sendskb+0x4c/0x6c ? netlink_unicast+0x28f/0x2ce ? rtnl_calcit.isra.0+0x150/0x146 netlink_rcv_skb+0x5f/0x112 netlink_unicast+0x213/0x2ce netlink_sendmsg+0x24f/0x4d9 __sock_sendmsg+0x65/0x6a ____sys_sendmsg+0x28f/0x2c9 ? import_iovec+0x17/0x2b ___sys_sendmsg+0x97/0xe0 __sys_sendmsg+0x81/0xd8 do_syscall_64+0x35/0x87 entry_SYSCALL_64_after_hwframe+0x6e/0x0 RIP: 0033:0x7fc328603727 Code: c3 66 90 41 54 41 89 d4 55 48 89 f5 53 89 fb 48 83 ec 10 e8 0b ed ff ff 44 89 e2 48 89 ee 89 df 41 89 c0 b8 2e 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 35 44 89 c7 48 89 44 24 08 e8 44 ed ff ff 48 RSP: 002b:00007ffe8eb3f1a0 EFLAGS: 00000293 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 000000000000000d RCX: 00007fc328603727 RDX: 0000000000000000 RSI: 00007ffe8eb3f1f0 RDI: 000000000000000d RBP:	N/A	More Details

	00007ffe8eb3f1f0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000293 R12: 0000000000000000 R13: 00000000000 ---truncated---		
CVE-2025-40251	In the Linux kernel, the following vulnerability has been resolved: devlink: rate: Unset parent pointer in devl_rate_nodes_destroy The function devl_rate_nodes_destroy is documented to "Unset parent for all rate objects". However, it was only calling the driver-specific `rate_leaf_parent_set` or `rate_node_parent_set` ops and decrementing the parent's refcount, without actually setting the `devlink_rate->parent` pointer to NULL. This leaves a dangling pointer in the `devlink_rate` struct, which cause refcount error in netdevsim[1] and mlx5[2]. In addition, this is inconsistent with the behavior of `devlink_nl_rate_parent_node_set`, where the parent pointer is correctly cleared. This patch fixes the issue by explicitly setting `devlink_rate->parent` to NULL after notifying the driver, thus fulfilling the function's documented behavior for all rate objects. [1] repro steps: echo 1 > /sys/bus/netdevsim/new_device devlink dev eswitch set netdevsim/netdevsim1 mode switchdev echo 1 > /sys/bus/netdevsim/devices/netdevsim1/sriov_numvfs devlink port function rate add netdevsim/netdevsim1/test_node devlink port function rate set netdevsim/netdevsim1/128 parent test_node echo 1 > /sys/bus/netdevsim/del_device dmesg: refcount_t: decrement hit 0; leaking memory. WARNING: CPU: 8 PID: 1530 at lib/refcount.c:31 refcount_warn_saturate+0x42/0xe0 CPU: 8 UID: 0 PID: 1530 Comm: bash Not tainted 6.18.0-rc4+ #1 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:refcount_warn_saturate+0x42/0xe0 Call Trace: <TASK> devl_rate_leaf_destroy+0x8d/0x90 __nsim_dev_port_del+0x6c/0x70 [netdevsim] nsim_dev_reload_destroy+0x11c/0x140 [netdevsim] nsim_drv_remove+0x2b/0xb0 [netdevsim] device_release_driver_internal+0x194/0x1f0 bus_remove_device+0xc6/0x130 device_del+0x159/0x3c0 device_unregister+0x1a/0x60 del_device_store+0x111/0x170 [netdevsim] kernfs_fop_write_iter+0x12e/0x1e0 vfs_write+0x215/0x3d0 ksys_write+0x5f/0xd0 do_syscall_64+0x55/0x10f0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [2] devlink dev eswitch set pci/0000:08:00.0 mode switchdev devlink port add pci/0000:08:00.0 flavour pcisf pfnum 0 sfnum 1000 devlink port function rate add pci/0000:08:00.0/group1 devlink port function rate set pci/0000:08:00.0/32768 parent group1 modprobe -r mlx5_ib mlx5_fwctl mlx5_core dmesg: refcount_t: decrement hit 0; leaking memory. WARNING: CPU: 7 PID: 16151 at lib/refcount.c:31 refcount_warn_saturate+0x42/0xe0 CPU: 7 UID: 0 PID: 16151 Comm: bash Not tainted 6.17.0-rc7_for_upstream_min_debug_2025_10_02_12_44 #1 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 RIP: 0010:refcount_warn_saturate+0x42/0xe0 Call Trace: <TASK> devl_rate_leaf_destroy+0x8d/0x90 mlx5_esw_offloads_devlink_port_unregister+0x33/0x60 [mlx5_core] mlx5_esw_offloads_unload_rep+0x3f/0x50 [mlx5_core] mlx5_eswitch_unload_sf_vport+0x40/0x90 [mlx5_core] mlx5_sf_esw_event+0xc4/0x120 [mlx5_core] notifier_call_chain+0x33/0xa0 blocking_notifier_call_chain+0x3b/0x50 mlx5_eswitch_disable_locked+0x50/0x110 [mlx5_core] mlx5_eswitch_disable+0x63/0x90 [mlx5_core] mlx5_unload+0x1d/0x170 [mlx5_core] mlx5_uninit_one+0xa2/0x130 [mlx5_core] remove_one+0x78/0xd0 [mlx5_core] pci_device_remove+0x39/0xa0 device_release_driver_internal+0x194/0x1f0 unbind_store+0x99/0xa0 kernfs_fop_write_iter+0x12e/0x1e0 vfs_write+0x215/0x3d0 ksys_write+0x5f/0xd0 do_syscall_64+0x53/0x1f0 entry_SYSCALL_64_after_hwframe+0x4b/0x53	N/A	More Details
CVE-2025-40252	In the Linux kernel, the following vulnerability has been resolved: net: qlogic/qede: fix potential out-of-bounds read in qede_tpa_cont() and qede_tpa_end() The loops in 'qede_tpa_cont()' and 'qede_tpa_end()', iterate over 'cqe->len_list[]' using only a zero-length terminator as the stopping condition. If the terminator was missing or malformed, the loop could run past the end of the fixed-size array. Add an explicit bound check using ARRAY_SIZE() in both loops to prevent a potential out-of-bounds access. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-63010	Server-Side Request Forgery (SSRF) vulnerability in ThemesInflow Hercules Core hercules-core allows Server Side Request Forgery.This issue affects Hercules Core : from n/a through <= 7.4.	N/A	More Details
CVE-2025-66456	Elysia is a Typescript framework for request validation, type inference, OpenAPI documentation and client-server communication. Versions 1.4.0 through 1.4.16 contain a prototype pollution vulnerability in `mergeDeep` after merging results of two standard schema validations with the same key. Due to the ordering of merging, there must be an any type that is set as a standalone guard, to allow for the `__proto__ prop` to be merged. When combined with GHSA-8vch-m3f4-q8jf this allows for a full RCE by an attacker. This issue is fixed in version 1.4.17. To workaround, remove the `__proto__ key` from body.	N/A	More Details
CVE-2025-40253	In the Linux kernel, the following vulnerability has been resolved: s390/ctcm: Fix double-kfree The function 'mpc_rcvd_sweep_req(mpcginfo)' is called conditionally from function 'ctcmpc_unpack_skb'. It frees passed mpcginfo. After that a call to function 'kfree' in function 'ctcmpc_unpack_skb' frees it again. Remove 'kfree' call in function 'mpc_rcvd_sweep_req(mpcginfo)'. Bug detected by the clang static analyzer.	N/A	More Details
CVE-2025-63011	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress WP Hotel Booking wp-hotel-booking allows DOM-Based XSS.This issue affects WP Hotel Booking: from n/a through <= 2.2.7.	N/A	More Details
CVE-2025-62997	Insertion of Sensitive Information Into Sent Data vulnerability in levelfourdevelopment WP EasyCart wp-easycart allows Retrieve Embedded Sensitive Data.This issue affects WP EasyCart: from n/a through <= 5.8.11.	N/A	More Details
CVE-2025-63009	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in yuvalo WP Google Analytics Events wp-google-analytics-events allows Retrieve Embedded Sensitive Data.This issue affects WP Google Analytics Events: from n/a through <= 2.8.2.	N/A	More Details
CVE-2023-53771	MiniDVBLinux 5.4 contains an authentication bypass vulnerability that allows remote attackers to change the root password without authentication. Attackers can send crafted POST requests to the system setup endpoint with modified SYSTEM_PASSWORD parameters to reset root credentials.	N/A	More Details
CVE-2025-62866	Cross-Site Request Forgery (CSRF) vulnerability in Valerio Monti Auto Alt Text auto-alt-text allows Cross Site Request Forgery.This issue affects Auto Alt Text: from n/a through <= 2.5.2.	N/A	More Details
CVE-2025-62865	Missing Authorization vulnerability in Evan Herman Post Cloner post-cloner allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post Cloner: from n/a through <= 1.0.0.	N/A	More Details
CVE-2023-53773	MiniDVBLinux 5.4 contains an unauthenticated vulnerability in the tv_action.sh script that allows remote attackers to generate live stream snapshots through the Simple VDR Protocol. Attackers can request /tpl/tv_action.sh to create and retrieve a live TV screenshot stored in /var/www/images/tv.jpg without authentication.	N/A	More Details
CVE-2023-53774	MiniDVBLinux 5.4 contains a remote code execution vulnerability in the SVDRP protocol that allows remote attackers to send commands to manipulate TV systems. Attackers can send crafted SVDRP commands through the svdrpsend.sh script to execute messages and potentially control the video disk recorder remotely.	N/A	More Details
CVE-	Cross-Site Request Forgery (CSRF) vulnerability in photoboxone SMTP Mail smtp-mail allows Cross Site Request Forgery.This issue affects		More

2025-62762	SMTP Mail: from n/a through <= 1.3.47.	N/A	Details
CVE-2025-13743	Docker Desktop diagnostics bundles were found to include expired Hub PATs in log output due to error object serialization. This poses a risk of leaking sensitive information in exported diagnostics, especially when access denied errors occurred.	N/A	More Details
CVE-2025-34425	MailEnable versions prior to 10.54 contain a reflected cross-site scripting (XSS) vulnerability in the WindowContext parameter of /Mondo/lang/sys/Forms/MAI/compose.aspx. The WindowContext value is not properly sanitized when processed via a GET request and is reflected within a <script> context in the JavaScript variable window.location, allowing an attacker to break out of the existing script and inject arbitrary JavaScript. A remote attacker can supply a crafted payload that terminates the existing ProcessContextSwitchResult() function, inserts attacker-controlled script, and comments out remaining code, leading to script execution in a victim's browser when the victim visits a malicious link or attempts to send an email. Successful exploitation can redirect victims to malicious sites, steal non-HttpOnly cookies, inject arbitrary HTML or CSS, and perform actions as the authenticated user.	N/A	More Details
CVE-2025-65513	fetch-mcp v1.0.2 and before is vulnerable to Server-Side Request Forgery (SSRF) vulnerability, which allows attackers to bypass private IP validation and access internal network resources.	N/A	More Details
CVE-2025-66039	FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. Versions are vulnerable to authentication bypass when the authentication type is set to "webserver." When providing an Authorization header with an arbitrary value, a session is associated with the target user regardless of valid credentials. This issue is fixed in versions 16.0.44 and 17.0.23.	N/A	More Details
CVE-2025-62740	Missing Authorization vulnerability in Mario Peshev WP-CRM System wp-crm-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP-CRM System: from n/a through <= 3.4.5.	N/A	More Details
CVE-2025-62739	Cross-Site Request Forgery (CSRF) vulnerability in SaifuMak Add Custom Codes add-custom-codes allows Cross Site Request Forgery.This issue affects Add Custom Codes: from n/a through <= 4.80.	N/A	More Details
CVE-2025-13760	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-62738	Missing Authorization vulnerability in mmattax Formstack Online Forms formstack allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Formstack Online Forms: from n/a through <= 2.0.2.	N/A	More Details
CVE-2025-62737	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in opicron Image Cleanup image-cleanup allows Retrieve Embedded Sensitive Data.This issue affects Image Cleanup: from n/a through <= 1.9.2.	N/A	More Details
CVE-2025-62736	Missing Authorization vulnerability in opicron Image Cleanup image-cleanup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Cleanup: from n/a through <= 1.9.2.	N/A	More Details
CVE-2025-62735	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Joel User Spam Remover user-spam-remover allows Retrieve Embedded Sensitive Data.This issue affects User Spam Remover: from n/a through <= 1.1.	N/A	More Details
CVE-2025-62734	Cross-Site Request Forgery (CSRF) vulnerability in Michael Revellin-Clerc Media Library Downloader media-library-downloader allows Cross Site Request Forgery.This issue affects Media Library Downloader: from n/a through <= 1.4.0.	N/A	More Details
CVE-2025-62733	Cross-Site Request Forgery (CSRF) vulnerability in ProteusThemes Custom Sidebars by ProteusThemes custom-sidebars-by-proteusthemes allows Cross Site Request Forgery.This issue affects Custom Sidebars by ProteusThemes: from n/a through <= 1.0.3.	N/A	More Details
CVE-2025-67497	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Details
CVE-2025-62153	Missing Authorization vulnerability in Graham Quick Interest Slider quick-interest-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Quick Interest Slider: from n/a through <= 3.1.5.	N/A	More Details
CVE-2025-62152	Missing Authorization vulnerability in ConveyThis ConveyThis conveythis-translate allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ConveyThis: from n/a through <= 268.10.	N/A	More Details
CVE-2025-62151	Missing Authorization vulnerability in Virtuaria Virtuaria PagBank / PagSeguro para Woocommerce virtuaria-pagseguro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Virtuaria PagBank / PagSeguro para Woocommerce: from n/a through <= 3.6.3.	N/A	More Details
CVE-2025-62109	Insertion of Sensitive Information Into Sent Data vulnerability in INFINITUM FORM Geo Controller cf-geoplugin allows Retrieve Embedded Sensitive Data.This issue affects Geo Controller: from n/a through <= 8.9.4.	N/A	More Details
CVE-2025-62103	Cross-Site Request Forgery (CSRF) vulnerability in wpmediadownload Media Library File Download media-download allows Cross Site Request Forgery.This issue affects Media Library File Download: from n/a through <= 1.4.	N/A	More Details
CVE-2025-62102	Cross-Site Request Forgery (CSRF) vulnerability in apasionados DoFollow Case by Case dofollow-case-by-case allows Cross Site Request Forgery.This issue affects DoFollow Case by Case: from n/a through <= 3.5.1.	N/A	More Details
CVE-	Missing Authorization vulnerability in themerain ThemeRain Core themerain-core allows Exploiting Incorrectly Configured Access Control		More

2025-62100	Security Levels.This issue affects ThemeRain Core: from n/a through <= 1.1.9.	N/A	Details
CVE-2025-62093	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Image&Video FullScreen Background lbg_fullscreen_fullwidth_slider allows SQL Injection.This issue affects Image&Video FullScreen Background: from n/a through <= 1.6.7.	N/A	More Details
CVE-2023-53772	MiniDVBLinux 5.4 contains an arbitrary file disclosure vulnerability that allows attackers to read sensitive system files through the 'file' GET parameter. Attackers can exploit the about page by supplying file paths to disclose arbitrary file contents on the affected device.	N/A	More Details
CVE-2023-53770	MiniDVBLinux 5.4 contains an unauthenticated configuration download vulnerability that allows remote attackers to access sensitive system configuration files through a direct object reference. Attackers can exploit the backup download endpoint by sending a GET request with 'action=getconfig' to retrieve a complete system configuration archive containing sensitive credentials.	N/A	More Details
CVE-2025-63008	Missing Authorization vulnerability in weDevs WP ERP erp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP ERP: from n/a through <= 1.16.7.	N/A	More Details
CVE-2023-53739	Tinycontrol LAN Controller v3 LK3 version 1.58a contains an unauthenticated vulnerability that allows remote attackers to download configuration backup files containing sensitive credentials. Attackers can retrieve the lk3_settings.bin file and extract base64-encoded user and admin passwords without authentication.	N/A	More Details
CVE-2025-63007	Insertion of Sensitive Information Into Sent Data vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Retrieve Embedded Sensitive Data.This issue affects EventPrime: from n/a through <= 4.2.4.1.	N/A	More Details
CVE-2025-63006	Missing Authorization vulnerability in Metagauss EventPrime eventprime-event-calendar-management allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EventPrime: from n/a through <= 4.2.4.1.	N/A	More Details
CVE-2025-63003	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes North - Required Plugin north-plugin allows PHP Local File Inclusion.This issue affects North - Required Plugin: from n/a through <= 1.4.2.	N/A	More Details
CVE-2025-62999	Missing Authorization vulnerability in themezaa Litho Addons litho-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Litho Addons: from n/a through <= 3.4.	N/A	More Details
CVE-2025-65287	An unauthenticated directory traversal vulnerability in cgi-bin/upload.cgi in SNMP Web Pro 1.1 allows a remote attacker to read arbitrary files. The CGI concatenates the user-supplied params directly onto the base path (/var/www/files/userScript/) using memcpy + strcat without validation or canonicalization, enabling ../ sequences to escape the intended directory. The download branch also echoes the unsanitized params into Content-Disposition, introducing header-injection risk.	N/A	More Details
CVE-2025-62996	Missing Authorization vulnerability in Code Amp Custom Layouts – Post + Product grids made easy custom-layouts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Custom Layouts – Post + Product grids made easy: from n/a through <= 1.4.12.	N/A	More Details
CVE-2025-62995	Missing Authorization vulnerability in multiparcels MultiParcels Shipping For WooCommerce multiparcels-shipping-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MultiParcels Shipping For WooCommerce: from n/a through <= 1.30.12.	N/A	More Details
CVE-2025-62994	Insertion of Sensitive Information Into Sent Data vulnerability in WP Messiah WP AI CoPilot ai-co-pilot-for-wp allows Retrieve Embedded Sensitive Data.This issue affects WP AI CoPilot: from n/a through <= 1.2.7.	N/A	More Details
CVE-2025-62993	Missing Authorization vulnerability in rainafarai Notification for Telegram notification-for-telegram allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Notification for Telegram: from n/a through <= 3.4.7.	N/A	More Details
CVE-2025-62873	Cross-Site Request Forgery (CSRF) vulnerability in Flashyapp WP Flashy Marketing Automation wp-flashy-marketing-automation allows Cross Site Request Forgery.This issue affects WP Flashy Marketing Automation: from n/a through <= 2.0.8.	N/A	More Details
CVE-2025-62872	Cross-Site Request Forgery (CSRF) vulnerability in JK Social Photo Fetcher facebook-photo-fetcher allows Cross Site Request Forgery.This issue affects Social Photo Fetcher: from n/a through <= 3.0.4.	N/A	More Details
CVE-2025-62871	Cross-Site Request Forgery (CSRF) vulnerability in Alex Prokopenko / JustCoded Just TinyMCE Custom Styles just-tinymce-styles allows Cross Site Request Forgery.This issue affects Just TinyMCE Custom Styles: from n/a through <= 1.2.1.	N/A	More Details
CVE-2021-47709	COMMAX Smart Home System allows an unauthenticated attacker to change configuration and cause denial-of-service through the setconf endpoint. Attackers can trigger a denial-of-service scenario by sending a malformed request to the setconf endpoint.	N/A	More Details
CVE-2021-47710	COMMAX Smart Home System is a smart IoT home solution that allows an unauthenticated attacker to disclose RTSP credentials in plain-text by exploiting the /overview.asp endpoint. Attackers can access sensitive information, including login credentials and DVR settings, by submitting a GET request to this endpoint.	N/A	More Details
CVE-2021-47717	IntelliChoice eFORCE Software Suite 2.5.9 contains a username enumeration vulnerability that allows attackers to enumerate valid users by exploiting the 'ctl00$MainContent$UserName' POST parameter. Attackers can send requests with valid usernames to retrieve user information.	N/A	More Details
CVE-2021-47718	OpenBMCS 2.4 contains an information disclosure vulnerability that allows unauthenticated attackers to access sensitive files by exploiting directory listing functionality. Attackers can browse directories like /debug/ and /php/ to discover configuration files, database credentials, and system information.	N/A	More Details

CVE-2025-62870	Missing Authorization vulnerability in Eupago Eupago Gateway For Woocommerce eupago-gateway-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Eupago Gateway For Woocommerce: from n/a through <= 4.6.3.	N/A	More Details
CVE-2025-62869	Missing Authorization vulnerability in Gravitec.net - Web Push Notifications Gravitec.net – Web Push Notifications gravitec-net-web-push-notifications allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gravitec.net – Web Push Notifications: from n/a through <= 2.9.17.	N/A	More Details
CVE-2025-62867	Missing Authorization vulnerability in ergonet Ergonet Cache ergonet-varnish-cache allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ergonet Cache: from n/a through <= 1.0.11.	N/A	More Details
CVE-2021-47719	COMMAX WebViewer ActiveX Control 2.1.4.5 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by providing excessively long string arrays through multiple functions. Attackers can exploit boundary errors in Commax_WebViewer.ocx to cause buffer overflow conditions and potentially gain code execution.	N/A	More Details
CVE-2021-47723	STVS ProVision 5.9.10 contains a cross-site request forgery vulnerability that allows attackers to perform actions with administrative privileges by exploiting unvalidated HTTP requests. Attackers can visit malicious web sites to trigger the forge request, allowing them to create new admin users.	N/A	More Details
CVE-2021-47724	STVS ProVision 5.9.10 contains a path traversal vulnerability that allows authenticated attackers to access arbitrary files by manipulating the files parameter in the archive download functionality. Attackers can send GET requests to /archive/download with directory traversal sequences to read sensitive system files like /etc/passwd.	N/A	More Details
CVE-2021-47727	Selea Targa IP OCR-ANPR Camera contains an unauthenticated vulnerability that allows remote attackers to access live video streams without authentication. Attackers can directly connect to RTP/RTSP or M-JPEG streams by requesting specific endpoints like p1.mjpg or p1.264 to view camera footage.	N/A	More Details
CVE-2021-47728	Selea Targa IP OCR-ANPR Camera contains an unauthenticated command injection vulnerability in utils.php that allows remote attackers to execute arbitrary shell commands. Attackers can exploit the 'addr' and 'port' parameters to inject commands and gain www-data user access through chained local file inclusion techniques.	N/A	More Details
CVE-2021-47729	Selea Targa IP OCR-ANPR Camera contains a stored cross-site scripting vulnerability in the 'files_list' parameter that allows attackers to inject malicious HTML and script code. Attackers can send a POST request to /cgi-bin/get_file.php with crafted payload to execute arbitrary scripts in victim's browser session.	N/A	More Details
CVE-2021-47730	Selea Targa IP OCR-ANPR Camera contains a cross-site request forgery vulnerability that allows attackers to create administrative users without authentication. Attackers can craft a malicious web page that submits a form to add a new admin user with full system privileges when a logged-in user visits the page.	N/A	More Details
CVE-2021-47731	Selea Targa IP OCR-ANPR Camera contains a hard-coded developer password vulnerability that allows unauthorized configuration access through an undocumented page. Attackers can exploit the hidden endpoint by using the hard-coded password 'Selea781830' to enable configuration upload and overwrite device settings.	N/A	More Details
CVE-2025-64696	Android App "Brother iPrint&Scan" versions 6.13.7 and earlier improperly uses an external cache directory. If exploited, application-specific files may be accessed from other malicious applications.	N/A	More Details
CVE-2025-66526	Missing Authorization vulnerability in Essekia Tablesome tablesome allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tablesome: from n/a through <= 1.1.34.	N/A	More Details
CVE-2025-66271	Clone for Windows provided by ELECOM CO.,LTD. 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-2025-40241	In the Linux kernel, the following vulnerability has been resolved: erofs: fix crafted invalid cases for encoded extents Robert recently reported two corrupted images that can cause system crashes, which are related to the new encoded extents introduced in Linux 6.15: - The first one [1] has plen != 0 (e.g. plen == 0x2000000) but (plen & Z_EROFS_EXTENT_PLEN_MASK) == 0. It is used to represent special extents such as sparse extents (!EROFS_MAP_MAPPED), but previously only plen == 0 was handled; - The second one [2] has pa 0xffffffffffdcffed and plen 0xb4000, then "cur [0xfffffffffffff000] += bvec.bv_len [0x1000]" in "} while ((cur += bvec.bv_len) < end);" wraps around, causing an out-of-bound access of pcl->compressed_bvecs[] in z_erofs_submit_queue(). EROFS only supports 48-bit physical block addresses (up to 1EiB for 4k blocks), so add a sanity check to enforce this.	N/A	More Details
CVE-2025-66453	Rhino is an open-source implementation of JavaScript written entirely in Java. Prior to 1.8.1, 1.7.15.1, and 1.7.14.1, when an application passed an attacker controlled float poing number into the toFixed() function, it might lead to high CPU consumption and a potential Denial of Service. Small numbers go through this call stack: NativeNumber.numTo > DToA.JS_dtostr > DToA.JS_dtoa > DToA.pow5mult where pow5mult attempts to raise 5 to a ridiculous power. This vulnerability is fixed in 1.8.1, 1.7.15.1, and 1.7.14.1.	N/A	More Details
CVE-2025-65097	RomM (ROM Manager) allows users to scan, enrich, browse and play their game collections with a clean and responsive interface. Prior to 4.4.1 and 4.4.1-beta.2, an Authenticated User can delete collections belonging to other users by directly sending a DELETE request to the collection endpoint. No ownership verification is performed before deleting collections. This vulnerability is fixed in 4.4.1 and 4.4.1-beta.2.	N/A	More Details
CVE-2025-65096	RomM (ROM Manager) allows users to scan, enrich, browse and play their game collections with a clean and responsive interface. Prior to 4.4.1 and 4.4.1-beta.2, users can read private collections / smart collections belonging to other users by directly accessing their IDs via API. No ownership verification or checking if the collection is public/private before returning collection data. This vulnerability is fixed in 4.4.1 and 4.4.1-beta.2.	N/A	More Details
CVE-2025-13086	Improper validation of source IP addresses in OpenVPN version 2.6.0 through 2.7_rc1 allows an attacker to open a session from a different IP address which did not initiate the connection resulting in a denial of service for the originating client	N/A	More Details
CVE-2025-12385	Allocation of Resources Without Limits or Throttling, Improper Validation of Specified Quantity in Input vulnerability in The Qt Company Qt on Windows, MacOS, Linux, iOS, Android, x86, ARM, 64 bit, 32 bit allows Excessive Allocation. This issue affects users of the Text component in Qt Quick. Missing validation of the width and height in the <img> tag could cause an application to become unresponsive. This issue affects Qt: from 5.0.0 through 6.5.10, from 6.6.0 through 6.8.5, from 6.9.0 through 6.10.0.	N/A	More Details
CVE-			

2025-12084	When building nested elements using xml.dom.minidom methods such as appendChild() that have a dependency on _clear_id_cache() the algorithm is quadratic. Availability can be impacted when building excessively nested documents.	N/A	More Details
CVE-2025-67573	Missing Authorization vulnerability in ThimPress Sailing sailing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sailing: from n/a through < 4.4.6.	N/A	More Details
CVE-2025-67572	Missing Authorization vulnerability in PenciDesign PenNews pennews allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PenNews: from n/a through < 6.7.4.	N/A	More Details
CVE-2025-67571	Missing Authorization vulnerability in WPFunnels WPFunnels wpfunnels allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPFunnels: from n/a through <= 3.6.2.	N/A	More Details
CVE-2025-67570	Missing Authorization vulnerability in GSheetConnector by WesternDeal WPForms Google Sheet Connector gsheetconnector-wpforms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPForms Google Sheet Connector: from n/a through <= 4.0.0.	N/A	More Details
CVE-2025-67569	Missing Authorization vulnerability in scriptsbundle AdForest adforest allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AdForest: from n/a through <= 6.0.11.	N/A	More Details
CVE-2025-67568	Missing Authorization vulnerability in xtemos Basel basel allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Basel: from n/a through <= 5.9.1.	N/A	More Details
CVE-2025-66478	Rejected reason: This CVE is a duplicate of CVE-2025-55182.	N/A	More Details
CVE-2025-64443	MCP Gateway allows easy and secure running and deployment of MCP servers. In versions 0.27.0 and earlier, when MCP Gateway runs in sse or streaming transport mode, it is vulnerable to DNS rebinding. An attacker who can get a victim to visit a malicious website or be served a malicious advertisement can perform browser-based exploitation of MCP servers executing behind the gateway, including manipulating tools or other features exposed by those MCP servers. MCP Gateway is not affected when running in the default stdio mode, which does not listen on network ports. Version 0.28.0 fixes this issue.	N/A	More Details
CVE-2025-64085	A NULL pointer dereference vulnerability in the importDataObject() function of PDF-XChange Editor v10.7.3.401 allows attackers to cause a Denial of Service (DoS) via a crafted input.	N/A	More Details
CVE-2025-64086	A NULL pointer dereference vulnerability in the util.readFileIntoStream component of PDF-XChange Editor v10.7.3.401 allows attackers to cause a Denial of Service (DoS) via a crafted input.	N/A	More Details
CVE-2025-34319	TOTOLINK N300RT wireless router firmware versions prior to V3.4.0-B20250430 (discovered in V2.1.8-B20201030.1539) contain an OS command injection vulnerability in the Boa formWsc handling functionality. An unauthenticated attacker can send specially crafted requests to trigger command execution via the targetAPSsid request parameter.	N/A	More Details
CVE-2025-40226	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Account for failed debug initialization When the SCMI debug subsystem fails to initialize, the related debug root will be missing, and the underlying descriptor will be NULL. Handle this fault condition in the SCMI debug helpers that maintain metrics counters.	N/A	More Details
CVE-2025-13751	Interactive service agent in OpenVPN version 2.5.0 through 2.7_rc2 on Windows allows a local authenticated user to connect to the service and trigger an error causing a local denial of service.	N/A	More Details
CVE-2025-40227	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: dealloc commit test ctx always The damon_ctx for testing online DAMON parameters commit inputs is deallocated only when the test fails. This means memory is leaked for every successful online DAMON parameters commit. Fix the leak by always deallocating it.	N/A	More Details
CVE-2025-67557	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rhys Wynne WP eBay Product Feeds ebay-feeds-for-wordpress allows Stored XSS.This issue affects WP eBay Product Feeds: from n/a through <= 3.4.9.	N/A	More Details
CVE-2025-67556	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHigh Advanced FAQ Manager advanced-faq-manager allows Stored XSS.This issue affects Advanced FAQ Manager: from n/a through <= 1.5.2.	N/A	More Details
CVE-2025-67555	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in useStrict UseStrict's Calendly Embedder cal-embedder-lite allows Stored XSS.This issue affects UseStrict's Calendly Embedder: from n/a through <= 1.1.7.2.	N/A	More Details
CVE-2025-67554	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Humanityco Cookie Notice & Compliance for GDPR / CCPA cookie-notice allows Stored XSS.This issue affects Cookie Notice & Compliance for GDPR / CCPA: from n/a through <= 2.5.8.	N/A	More Details
CVE-2025-67553	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHigh Advanced FAQ Manager advanced-faq-manager allows DOM-Based XSS.This issue affects Advanced FAQ Manager: from n/a through <= 1.5.2.	N/A	More Details
CVE-2025-67552	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WalkerWP Walker Core walker-core allows DOM-Based XSS.This issue affects Walker Core: from n/a through <= 1.3.17.	N/A	More Details
CVE-2025-67551	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wappointment team Wappointment wappointment allows Stored XSS.This issue affects Wappointment: from n/a through <= 2.6.9.	N/A	More Details

CVE-2025-67550	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rhewlif Donation Thermometer donation-thermometer allows Stored XSS.This issue affects Donation Thermometer: from n/a through <= 2.2.6.	N/A	More Details
CVE-2025-67549	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bobbingwide oik oik allows DOM-Based XSS.This issue affects oik: from n/a through <= 4.15.3.	N/A	More Details
CVE-2025-66489	Cal.com is open-source scheduling software. Prior to 5.9.8, A flaw in the login credentials provider allows an attacker to bypass password verification when a TOTP code is provided, potentially gaining unauthorized access to user accounts. This issue exists due to problematic conditional logic in the authentication flow. This vulnerability is fixed in 5.9.8.	N/A	More Details
CVE-2025-62173	## Summary Authenticated SQL Injection Vulnerability in Endpoint Module Rest API	N/A	More Details
CVE-2025-40214	In the Linux kernel, the following vulnerability has been resolved: af_unix: Initialise scc_index in unix_add_edge(). Quang Le reported that the AF_UNIX GC could garbage-collect a receive queue of an alive in-flight socket, with a nice repro. The repro consists of three stages. 1) 1-a. Create a single cyclic reference with many sockets 1-b. close() all sockets 1-c. Trigger GC 2) 2-a. Pass sk-A to an embryo sk-B 2-b. Pass sk-X to sk-X 2-c. Trigger GC 3) 3-a. accept() the embryo sk-B 3-b. Pass sk-B to sk-C 3-c. close() the in-flight sk-A 3-d. Trigger GC As of 2-c, sk-A and sk-X are linked to unix_unvisited_vertices, and unix_walk_scc() groups them into two different SCCs: unix_sk(sk-A)->vertex->scc_index = 2 (UNIX_VERTEX_INDEX_START) unix_sk(sk-X)->vertex->scc_index = 3 Once GC completes, unix_graph_grouped is set to true. Also, unix_graph_maybe_cyclic is set to true due to sk-X's cyclic self-reference, which makes close() trigger GC. At 3-b, unix_add_edge() allocates unix_sk(sk-B)->vertex and links it to unix_unvisited_vertices. unix_update_graph() is called at 3-a. and 3-b., but neither unix_graph_grouped nor unix_graph_maybe_cyclic is changed because both sk-B's listener and sk-C are not in-flight. 3-c decrements sk-A's file refcnt to 1. Since unix_graph_grouped is true at 3-d, unix_walk_scc_fast() is finally called and iterates 3 sockets sk-A, sk-B, and sk-X: sk-A -> sk-B (-> sk-C) sk-X -> sk-X This is totally fine. All of them are not yet close()d and should be grouped into different SCCs. However, unix_vertex_dead() misjudges that sk-A and sk-B are in the same SCC and sk-A is dead. unix_sk(sk-A)->scc_index == unix_sk(sk-B)->scc_index <-- Wrong! && sk-A's file refcnt == unix_sk(sk-A)->vertex->out_degree ^-- 1 in-flight count for sk-B -> sk-A is dead !? The problem is that unix_add_edge() does not initialise scc_index. Stage 1) is used for heap spraying, making a newly allocated vertex have vertex->scc_index == 2 (UNIX_VERTEX_INDEX_START) set by unix_walk_scc() at 1-c. Let's track the max SCC index from the previous unix_walk_scc() call and assign the max + 1 to a new vertex's scc_index. This way, we can continue to avoid Tarjan's algorithm while preventing misjudgments.	N/A	More Details
CVE-2025-9638	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Portabilis i-Educar allows Stored Cross-Site Scripting (XSS) via the matricula_interna parameter in the educar_usuario_cad.php endpoint. This issue affects i-Educar: 2.10.0.	N/A	More Details
CVE-2025-40225	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix kernel panic on partial unmap of a GPU VA region This commit address a kernel panic issue that can happen if Userspace tries to partially unmap a GPU virtual region (aka drm_gpuva). The VM_BIND interface allows partial unmapping of a BO. Panthor driver pre-allocates memory for the new drm_gpuva structures that would be needed for the map/unmap operation, done using drm_gpuvm layer. It expected that only one new drm_gpuva would be needed on umap but a partial unmap can require 2 new drm_gpuva and that's why it ended up doing a NULL pointer dereference causing a kernel panic. Following dump was seen when partial unmap was exercised. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000078 Mem abort info: ESR = 0x0000000096000046 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 = 0x00000046, ISS2 = 0x00000000 CM = 0, WnR = 1, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=000000088a863000 [0000000000000078] pgd=080000088a842003, p4d=080000088a842003, pud=0800000884bf5003, pmd=0000000000000000 Internal error: Oops: 0000000096000046 [#1] PREEMPT SMP <snip> pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : panthor_gpuva_sm_step_remap+0xe4/0x330 [panthor] lr : panthor_gpuva_sm_step_remap+0x6c/0x330 [panthor] sp : ffff800085d43970 x29: ffff800085d43970 x28: ffff00080363e440 x27: ffff0008090c6000 x26: 0000000000000030 x25: ffff800085d439f8 x24: ffff00080d402000 x23: ffff800085d43b60 x22: ffff800085d439e0 x21: ffff00080abdb180 x20: 0000000000000000 x19: 0000000000000000 x18: 0000000000000010 x17: 6e656c202c303030 x16: 3666666666646466 x15: 393d61766f69202c x14: 312d3d7361203a70 x13: 303030323d6e656c x12: ffff80008324bf58 x11: 0000000000000003 x10: 0000000000000002 x9 : ffff8000801a6a9c x8 : ffff00080360b300 x7 : 0000000000000000 x6 : 000000088aa35fc7 x5 : fff1000080000000 x4 : ffff8000842ddd30 x3 : 0000000000000001 x2 : 0000000100000000 x1 : 0000000000000001 x0 : 0000000000000078 Call trace: panthor_gpuva_sm_step_remap+0xe4/0x330 [panthor] op_remap_cb.isra.22+0x50/0x80 __drm_gpuvm_sm_unmap+0x10c/0x1c8 drm_gpuvm_sm_unmap+0x40/0x60 panthor_vm_exec_op+0xb4/0x3d0 [panthor] panthor_vm_bind_exec_sync_op+0x154/0x278 [panthor] panthor_ioctl_vm_bind+0x160/0x4a0 [panthor] drm_ioctl_kernel+0xbc/0x138 drm_ioctl+0x240/0x500 __arm64_sys_ioctl+0xb0/0xf8 invoke_syscall+0x4c/0x110 el0_svc_common.constprop.1+0x98/0xf8 do_el0_svc+0x24/0x38 el0_svc+0x40/0xf8 el0t_64_sync_handler+0xa0/0xc8 el0t_64_sync+0x174/0x178	N/A	More Details
CVE-2025-63742	SQL Injection vulnerability in function setwxqyAction in file webmain/task/api/loginAction.php in Xinhu Rainrock RockOA 2.7.0 allowing attackers gain sensitive information, including administrator accounts, password hashes, database structure, and other critical data via the shouji and userid parameters.	N/A	More Details
CVE-2025-63740	SQL Injection vulnerability in function getselectdataAjax in file inputAction.php in Xinhu Rainrock RockOA 2.7.0 allowing attackers gain sensitive information, including administrator accounts, password hashes, database structure, and other critical data via the actstr parameter.	N/A	More Details
CVE-2025-63739	An issue was discovered in function phpinisaveAction in file webmain/system/cogini/coginiAction.php in Xinhu Rainrock RockOA 2.7.0 allowing attackers to authenticated users to modify PHP configuration files via the a parameter to the index.php endpoint.	N/A	More Details
CVE-2025-63738	An issue was discovered in file index.php in Xinhu Rainrock RockOA 2.7.0 allowing attackers to gain sensitive information via phpinfo via the a parameter to the index.php.	N/A	More Details
CVE-2025-63737	Cross-site scripting (XSS) vulnerability in function urltestAction in file cliAction.php in Xinhu Rainrock RockOA 2.7.0 allows remote attackers to inject arbitrary web script or HTML via the m parameter to the task.php endpoint.	N/A	More Details
CVE-2025-56704	LeptonCMS version 7.3.0 contains an arbitrary file upload vulnerability, which is caused by the lack of proper validation for uploaded files. An authenticated attacker can exploit this vulnerability by uploading a specially crafted ZIP/PHP file to execute arbitrary code.	N/A	More Details

CVE-2025-12946	A vulnerability in the speedtest feature of affected NETGEAR Nighthawk routers, caused by improper input validation, can allow attackers on the router's WAN side, using attacker-in-the-middle techniques (MiTM) to manipulate DNS responses and execute commands when speedtests are run. This issue affects RS700: through 1.0.7.82; RAX54Sv2 : before V1.1.6.36; RAX41v2: before V1.1.6.36; RAX50: before V1.2.14.114; RAXE500: before V1.2.14.114; RAX41: before V1.0.17.142; RAX43: before V1.0.17.142; RAX35v2: before V1.0.17.142; RAXE450: before V1.2.14.114; RAX43v2: before V1.1.6.36; RAX42: before V1.0.17.142; RAX45: before V1.0.17.142; RAX50v2: before V1.1.6.36; MR90: before V1.0.2.46; MS90: before V1.0.2.46; RAX42v2: before V1.1.6.36; RAX49S: before V1.1.6.36.	N/A	More Details
CVE-2025-12945	A vulnerability in NETGEAR Nighthawk R7000P routers lets an authenticated admin execute OS command injections due to improper input validation. This issue affects R7000P: through 1.3.3.154.	N/A	More Details
CVE-2025-12941	Denial of Service Vulnerability in NETGEAR C6220 and C6230 (DOCSIS® 3.0 Two-in-one Cable Modem + WiFi Router) allows authenticated local WiFi users reboot the router.	N/A	More Details
CVE-2025-40224	In the Linux kernel, the following vulnerability has been resolved: hwmon: (cgbc-hwmon) Add missing NULL check after devm_kzalloc() The driver allocates memory for sensor data using devm_kzalloc(), but did not check if the allocation succeeded. In case of memory allocation failure, dereferencing the NULL pointer would lead to a kernel crash. Add a NULL pointer check and return -ENOMEM to handle allocation failure properly.	N/A	More Details
CVE-2025-40223	In the Linux kernel, the following vulnerability has been resolved: most: usb: Fix use-after-free in hdm_disconnect hdm_disconnect() calls most_deregister_interface(), which eventually unregisters the MOST interface device with device_unregister(iface->dev). If that drops the last reference, the device core may call release_mdev() immediately while hdm_disconnect() is still executing. The old code also freed several mdev-owned allocations in hdm_disconnect() and then performed additional put_device() calls. Depending on refcount order, this could lead to use-after-free or double-free when release_mdev() ran (or when unregister paths also performed puts). Fix by moving the frees of mdev-owned allocations into release_mdev(), so they happen exactly once when the device is truly released, and by dropping the extra put_device() calls in hdm_disconnect() that are redundant after device_unregister() and most_deregister_interface(). This addresses the KASAN slab-use-after-free reported by syzbot in hdm_disconnect(). See report and stack traces in the bug link below.	N/A	More Details
CVE-2025-34396	MailEnable versions prior to 10.54 contain an unsafe DLL loading vulnerability that can lead to local arbitrary code execution. The MailEnable administrative executable attempts to load MEAINFY.DLL from its application directo without sufficient integrity validation or secure search order. If the DLL is missing or attacker-writable locations in the search path are used, a local attacker with write permissions to the directory can plant a malicious MEAINFY.DLL. When the executable is launched, it loads the attacker-controlled library and executes code with the privileges of the process, enabling local privilege escalation when run with elevated rights.	N/A	More Details
CVE-2025-9368	A security issue exists within 432ES-IG3 Series A, which affects GuardLink® EtherNet/IP Interface, resulting in denial-of-service. A manual power cycle is required to recover the device.	N/A	More Details
CVE-2025-40215	In the Linux kernel, the following vulnerability has been resolved: xfrm: delete x->tunnel as we delete x The ipcomp fallback tunnels currently get deleted (from the various lists and hashtables) as the last user state that needed that fallback is destroyed (not deleted). If a reference to that user state still exists, the fallback state will remain on the hashtables/lists, triggering the WARN in xfrm_state_fini. Because of those remaining references, the fix in commit f75a2804da39 ("xfrm: destroy xfrm_state synchronously on net exit path") is not complete. We recently fixed one such situation in TCP due to defered freeing of skbs (commit 9b6412e6979f ("tcp: drop secpath at the same time as we currently drop dst")). This can also happen due to IP reassembly: skbs with a secpath remain on the reassembly queue until netns destruction. If we can't guarantee that the queues are flushed by the time xfrm_state_fini runs, there may still be references to a (user) xfrm_state, preventing the timely deletion of the corresponding fallback state. Instead of chasing each instance of skbs holding a secpath one by one, this patch fixes the issue directly within xfrm, by deleting the fallback state as soon as the last user state depending on it has been deleted. Destruction will still happen when the final reference is dropped. A separate lockdep class for the fallback state is required since we're going to lock x->tunnel while x is locked.	N/A	More Details
CVE-2025-62086	Missing Authorization vulnerability in akazanstev Яндекс Доставка (Boxberry) boxberry allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Яндекс Доставка (Boxberry): from n/a through <= 2.32.	N/A	More Details
CVE-2025-34413	Legality WHISTLEBLOWING by DigitalPA contains a protection mechanism failure in which critical HTTP security headers are not emitted by default. Affected deployments omit Content-Security-Policy, Referrer-Policy, Permissions-Policy, Cross-Origin-Embedder-Policy, Cross-Origin-Opener-Policy, and Cross-Origin-Resource-Policy (with CSP delivered via HTML meta elements being inadequate). The absence of these headers weakens browser-side defenses and increases exposure to client-side attacks such as cross-site scripting, clickjacking, referer leakage, and cross-origin data disclosure.	N/A	More Details
CVE-2025-34414	Entrust Instant Financial Issuance (IFI) On Premise software (formerly referred to as CardWizard) versions 5.x, prior to 6.10.5, and prior to 6.11.1 contain an insecure .NET Remoting exposure in the Legacy Remoting Service that is enabled by default. The service registers a TCP remoting channel with SOAP and binary formatters configured at TypeFilterLevel=Full and exposes default ObjectURI endpoints. A remote, unauthenticated attacker who can reach the remoting port can invoke the exposed remoting objects to read arbitrary files from the server and coerce outbound authentication, and may achieve arbitrary file write and remote code execution via known .NET Remoting exploitation techniques. This can lead to disclosure of sensitive installation and service-account data and compromise of the affected host.	N/A	More Details
CVE-2025-40222	In the Linux kernel, the following vulnerability has been resolved: tty: serial: sh-sci: fix RSCI FIFO overrun handling The receive error handling code is shared between RSCI and all other SCIF port types, but the RSCI overrun_reg is specified as a memory offset, while for other SCIF types it is an enum value used to index into the sci_port_params->regs array, as mentioned above the sci_serial_in() function. For RSCI, the overrun_reg is CSR (0x48), causing the sci_getreg() call inside the sci_handle_fifo_overrun() function to index outside the bounds of the regs array, which currently has a size of 20, as specified by SCI_NR_REGS. Because of this, we end up accessing memory outside of RSCI's rsci_port_params structure, which, when interpreted as a plat_sci_reg, happens to have a non-zero size, causing the following WARN when sci_serial_in() is called, as the accidental size does not match the supported register sizes. The existence of the overrun_reg needs to be checked because SCIx_SH3_SCIF_REGTYPE has overrun_reg set to SCLSR, but SCLSR is not present in the regs array. Avoid calling sci_getreg() for port types which don't use standard register handling. Use the ops->read_reg() and ops->write_reg() functions to properly read and write registers for RSCI, and change the type of the status variable to accommodate the 32-bit CSR register. sci_getreg() and sci_serial_in() are also called with overrun_reg in the sci_mpxed_interrupt() interrupt handler, but that code path is not used for RSCI, as it does not have a muxed interrupt. ------------[cut here]------------ Invalid register access WARNING: CPU: 0 PID: 0 at drivers/tty/serial/sh-sci.c:522 sci_serial_in+0x38/0xac Modules linked in: renesas_usbhs at24 rzt2h_adc industrialio_adc sha256 cfg80211 bluetooth ecdh_generic ecc rfkill fuse drm backlight ipv6 CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Not tainted 6.17.0-rc1+ #30 PREEMPT Hardware name: Renesas RZ/T2H EVK Board based on r9a09g077m44 (DT) pstate: 604000c5 (nZCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : sci_serial_in+0x38/0xac lr : sci_serial_in+0x38/0xac sp : ffff800080003e80 x29: ffff800080003e80 x28: ffff800082195b80 x27: 000000000000000d x26: ffff8000821956d0 x25: 0000000000000000 x24: ffff800082195b80 x23: ffff000180e0d800 x22: 0000000000000010 x21: 0000000000000000 x20: 0000000000000010 x19: ffff000180e72000 x18: 000000000000000a x17:	N/A	More Details

	ffff8002bcee7000 x16: ffff800080000000 x15: 0720072007200720 x14: 0720072007200720 x13: 0720072007200720 x12: 0720072007200720 x11: 0000000000000058 x10: 0000000000000018 x9 : ffff8000821a6a48 x8 : 0000000000057fa8 x7 : 0000000000000406 x6 : ffff8000821fea48 x5 : ffff00033ef88408 x4 : ffff8002bcee7000 x3 : ffff800082195b80 x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff800082195b80 Call trace: sci_serial_in+0x38/0xac (P) sci_handle_fifo_overrun.isra.0+0x70/0x134 sci_er_interrupt+0x50/0x39c __handle_irq_event_percpu+0x48/0x140 handle_irq_event+0x44/0xb0 handle_fasteoi_irq+0xf4/0x1a0 handle_irq_desc+0x34/0x58 generic_handle_domain_irq+0x1c/0x28 gic_handle_irq+0x4c/0x140 call_on_irq_stack+0x30/0x48 do_interrupt_handler+0x80/0x84 el1_interrupt+0x34/0x68 el1h_64_irq_handler+0x18/0x24 el1h_64_irq+0x6c/0x70 default_idle_call+0x28/0x58 (P) do_idle+0x1f8/0x250 cpu_startup_entry+0x34/0x3c rest_init+0xd8/0xe0 console_on_rootfs+0x0/0x6c __primary_switched+0x88/0x90 ---[end trace 0000000000000000]---		
CVE-2025-14024	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-40221	In the Linux kernel, the following vulnerability has been resolved: media: pci: mg4b: fix uninitialized iio scan data Fix potential leak of uninitialized stack data to userspace by ensuring that the `scan` structure is zeroed before use.	N/A	More Details
CVE-2025-40220	In the Linux kernel, the following vulnerability has been resolved: fuse: fix livelock in synchronous file put from fuseblk workers I observed a hang when running generic/323 against a fuseblk server. This test opens a file, initiates a lot of AIO writes to that file descriptor, and closes the file descriptor before the writes complete. Unsurprisingly, the AIO exerciser threads are mostly stuck waiting for responses from the fuseblk server: # cat /proc/372265/task/372313/stack [<0>] request_wait_answer+0x1fe/0x2a0 [fuse] [<0>] __fuse_simple_request+0xd3/0x2b0 [fuse] [<0>] fuse_do_getattr+0xfc/0x1f0 [fuse] [<0>] fuse_file_read_iter+0xbe/0x1c0 [fuse] [<0>] aio_read+0x130/0x1e0 [<0>] io_submit_one+0x542/0x860 [<0>] __x64_sys_io_submit+0x98/0x1a0 [<0>] do_syscall_64+0x37/0xf0 [<0>] entry_SYSCALL_64_after_hwframe+0x4b/0x53 But the /weird/ part is that the fuseblk server threads are waiting for responses from itself: # cat /proc/372210/task/372232/stack [<0>] request_wait_answer+0x1fe/0x2a0 [fuse] [<0>] __fuse_simple_request+0xd3/0x2b0 [fuse] [<0>] fuse_file_put+0x9a/0xd0 [fuse] [<0>] fuse_release+0x36/0x50 [fuse] [<0>] __fput+0xec/0x2b0 [<0>] task_work_run+0x55/0x90 [<0>] syscall_exit_to_user_mode+0xe9/0x100 [<0>] do_syscall_64+0x43/0xf0 [<0>] entry_SYSCALL_64_after_hwframe+0x4b/0x53 The fuseblk server is fuse2fs so there's nothing all that exciting in the server itself. So why is the fuse server calling fuse_file_put? The commit message for the fstest sheds some light on that: "By closing the file descriptor before calling io_destroy, you pretty much guarantee that the last put on the ioctx will be done in interrupt context (during I/O completion). Aha. AIO fgets a new struct file from the fd when it queues the ioctx. The completion of the FUSE_WRITE command from userspace causes the fuse server to call the AIO completion function. The completion puts the struct file, queuing a delayed fput to the fuse server task. When the fuse server task returns to userspace, it has to run the delayed fput, which in the case of a fuseblk server, it does synchronously. Sending the FUSE_RELEASE command sychronously from fuse server threads is a bad idea because a client program can initiate enough simultaneous AIOs such that all the fuse server threads end up in delayed_fput, and now there aren't any threads left to handle the queued fuse commands. Fix this by only using asynchronous fputs when closing files, and leave a comment explaining why.	N/A	More Details
CVE-2025-40219	In the Linux kernel, the following vulnerability has been resolved: PCI/IOV: Add PCI rescan-remove locking when enabling/disabling SR-IOV Before disabling SR-IOV via config space accesses to the parent PF, sriov_disable() first removes the PCI devices representing the VFs. Since commit 9d16947b7583 ("PCI: Add global pci_lock_rescan_remove()") such removal operations are serialized against concurrent remove and rescan using the pci_rescan_remove_lock. No such locking was ever added in sriov_disable() however. In particular when commit 18f9e9d150fc ("PCI/IOV: Factor out sriov_add_vfs()") factored out the PCI device removal into sriov_del_vfs() there was still no locking around the pci_iov_remove_virtfn() calls. On s390 the lack of serialization in sriov_disable() may cause double remove and list corruption with the below (amended) trace being observed: PSW: 0704c00180000000 0000000c914e4b38 (klist_put+56) GPRS: 000003800313fb48 0000000000000000 0000000100000001 0000000000000001 00000000f9b520a8 0000000000000000 0000000000002fbd 00000000f4cc9480 0000000000000001 0000000000000000 0000000000000000 0000000180692828 00000000818e8000 000003800313fe2c 000003800313fb20 000003800313fad8 #0 [3800313fb20] device_del at c9158ad5c #1 [3800313fb88] pci_remove_bus_device at c915105ba #2 [3800313fbd0] pci_iov_remove_virtfn at c9152f198 #3 [3800313fc28] zpci_iov_remove_virtfn at c90fb67c0 #4 [3800313fc60] zpci_bus_remove_device at c90fb6104 #5 [3800313fca0] __zpci_event_availability at c90fb3dca #6 [3800313fd08] chsc_process_sei_nt0 at c918fe4a2 #7 [3800313fd60] crw_collect_info at c91905822 #8 [3800313fe10] kthread at c90feb390 #9 [3800313fe68] __ret_from_fork at c90f6aa64 #10 [3800313fe98] ret_from_fork at c9194f3f2. This is because in addition to sriov_disable() removing the VFs, the platform also generates hot-unplug events for the VFs. This being the reverse operation to the hotplug events generated by sriov_enable() and handled via pdev->no_vf_scan. And while the event processing takes pci_rescan_remove_lock and checks whether the struct pci_dev still exists, the lack of synchronization makes this checking racy. Other races may also be possible of course though given that this lack of locking persisted so long observable races seem very rare. Even on s390 the list corruption was only observed with certain devices since the platform events are only triggered by config accesses after the removal, so as long as the removal finished synchronously they would not race. Either way the locking is missing so fix this by adding it to the sriov_del_vfs() helper. Just like PCI rescan-remove, locking is also missing in sriov_add_vfs() including for the error case where pci_stop_and_remove_bus_device() is called without the PCI rescan-remove lock being held. Even in the non-error case, adding new PCI devices and buses should be serialized via the PCI rescan-remove lock. Add the necessary locking.	N/A	More Details
CVE-2025-40218	In the Linux kernel, the following vulnerability has been resolved: mm/damon/vaddr: do not repeat pte_offset_map_lock() until success DAMON's virtual address space operation set implementation (vaddr) calls pte_offset_map_lock() inside the page table walk callback function. This is for reading and writing page table accessed bits. If pte_offset_map_lock() fails, it retries by returning the page table walk callback function with ACTION_AGAIN. pte_offset_map_lock() can continuously fail if the target is a pmd migration entry, though. Hence it could cause an infinite page table walk if the migration cannot be done until the page table walk is finished. This indeed caused a soft lockup when CPU hotplugging and DAMON were running in parallel. Avoid the infinite loop by simply not retrying the page table walk. DAMON is promising only a best-effort accuracy, so missing access to such pages is no problem.	N/A	More Details
CVE-2025-40217	In the Linux kernel, the following vulnerability has been resolved: pidfs: validate extensible ioctls Validate extensible ioctls stricter than we do now.	N/A	More Details
CVE-2025-40216	In the Linux kernel, the following vulnerability has been resolved: io_uring/rsrc: don't rely on user vaddr alignment There is no guaranteed alignment for user pointers, however the calculation of an offset of the first page into a folio after coalescing uses some weird bit mask logic, get rid of it.	N/A	More Details
CVE-2025-61078	Cross-site scripting (XSS) vulnerability in Request IP form in phpIPAM v1.7.3 allows remote attackers to inject arbitrary web script or HTML via the instructions parameter for the /app/admin/instructions/edit-result.php endpoint.	N/A	More Details
CVE-2025-61258	An issue was discovered in Outsystems Platform Server 11.18.1.37828 allows attackers to cause a denial of service via crafted content-length value mismatching the body length.	N/A	More Details

CVE-2025-67548	Missing Authorization vulnerability in WP Delicious WP Delicious delicious-recipes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Delicious: from n/a through <= 1.9.1.	N/A	More Details
CVE-2025-67545	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FirePlugins FireBox firebox allows Stored XSS.This issue affects FireBox: from n/a through <= 3.1.0-free.	N/A	More Details
CVE-2025-40228	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: catch commit test ctx alloc failure Patch series "mm/damon/sysfs: fix commit test damon_ctx [de]allocation". DAMON sysfs interface dynamically allocates and uses a damon_ctx object for testing if given inputs for online DAMON parameters update is valid. The object is being used without an allocation failure check, and leaked when the test succeeds. Fix the two bugs. This patch (of 2): The damon_ctx for testing online DAMON parameters commit inputs is used without its allocation failure check. This could result in an invalid memory access. Fix it by directly returning an error when the allocation failed.	N/A	More Details
CVE-2025-65572	Cross Site Scripting (XSS) vulnerability in AllskyTeam AllSky v2024.12.06_06 allows remote attackers to execute arbitrary code via the (1) config, (2) filename, or (3) extratext parameter to allskySettings.php. When the page is reloaded or when user visits allskySettings.php, the showMessages() function in status_messages.php will print out the error messages and execute the script injected by the attacker.	N/A	More Details
CVE-2025-67473	Cross-Site Request Forgery (CSRF) vulnerability in codeworkweb CWW Companion cww-companion allows Cross Site Request Forgery.This issue affects CWW Companion: from n/a through <= 1.3.2.	N/A	More Details
CVE-2025-67472	Cross-Site Request Forgery (CSRF) vulnerability in vcita Online Booking & Scheduling Calendar for WordPress by vcita meeting-scheduler-by-vcita allows Cross Site Request Forgery.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through <= 4.5.5.	N/A	More Details
CVE-2025-67471	Cross-Site Request Forgery (CSRF) vulnerability in Saad Iqbal Quick Contact Form quick-contact-form allows Cross Site Request Forgery.This issue affects Quick Contact Form: from n/a through <= 8.2.5.	N/A	More Details
CVE-2025-67470	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Essential Plugin Portfolio and Projects portfolio-and-projects allows Retrieve Embedded Sensitive Data.This issue affects Portfolio and Projects: from n/a through <= 1.5.5.	N/A	More Details
CVE-2025-67469	Cross-Site Request Forgery (CSRF) vulnerability in kubiq PDF Thumbnail Generator pdf-thumbnail-generator allows Cross Site Request Forgery.This issue affects PDF Thumbnail Generator: from n/a through <= 1.4.	N/A	More Details
CVE-2025-67468	Missing Authorization vulnerability in CRM Perks Integration for Salesforce and Contact Form 7, WPForms, Elementor, Formidable, Ninja Forms cf7-salesforce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Integration for Salesforce and Contact Form 7, WPForms, Elementor, Formidable, Ninja Forms: from n/a through <= 1.4.6.	N/A	More Details
CVE-2025-65300	A stored Cross-Site Scripting (XSS) vulnerability exists in the Coohom SaaS Platform feVersion=1760060603897 (2025-10-28) in the Account Settings module, where unsanitized user input in Address fields (City, State, Country/Region) is rendered back to the page. Attackers can inject arbitrary JavaScript code, which executes when the affected profile page is viewed. This can lead to session hijacking, cookie theft, or arbitrary script execution in the victim's browser.	N/A	More Details
CVE-2025-67466	Missing Authorization vulnerability in sergiotrinity Trinity Audio trinity-audio allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Trinity Audio: from n/a through <= 5.23.3.	N/A	More Details
CVE-2025-67465	Cross-Site Request Forgery (CSRF) vulnerability in QuantumCloud Simple Link Directory simple-link-directory allows Cross Site Request Forgery.This issue affects Simple Link Directory: from n/a through <= 8.8.3.	N/A	More Details
CVE-2025-66649	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Details
CVE-2025-66631	CSLA .NET is a framework designed for the development of reusable, object-oriented business layers for applications. Versions 5.5.4 and below allow the use of WcfProxy. WcfProxy uses the now-obsolete NetDataContractSerializer (NDCS) and is vulnerable to remote code execution during deserialization. This vulnerability is fixed in version 6.0.0. To workaround this issue, remove the WcfProxy in data portal configurations.	N/A	More Details
CVE-2025-40238	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix IPsec cleanup over MPV device When we do mlx5e_detach_netdev() we eventually disable blocking events notifier, among those events are IPsec MPV events from IB to core. So before disabling those blocking events, make sure to also unregister the devcom device and mark all this device operations as complete, in order to prevent the other device from using invalid netdev during future devcom events which could cause the trace below. BUG: kernel NULL pointer dereference, address: 0000000000000010 PGD 146427067 P4D 146427067 PUD 146488067 PMD 0 Oops: Oops: 0000 [#1] SMP CPU: 1 UID: 0 PID: 7735 Comm: devlink Tainted: GW 6.12.0-rc6_for_upstream_min_debug_2024_11_08_00_46 #1 Tainted: [W]=WARN Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 RIP: 0010:mlx5_devcom_comp_set_ready+0x5/0x40 [mlx5_core] Code: 00 01 48 83 05 23 32 1e 00 01 41 b8 ed ff ff ff e9 60 ff ff ff 48 83 05 00 32 1e 00 01 eb e3 66 0f 1f 44 00 00 0f 1f 44 00 00 <48> 8b 47 10 48 83 05 5f 32 1e 00 01 48 8b 50 40 48 85 d2 74 05 40 RSP: 0018:ffff88811a5c35f8 EFLAGS: 00010206 RAX: ffff888106e8ab80 RBX: ffff888107d7e200 RCX: ffff88810d6f0a00 RDX: ffff88810d6f0a00 RSI: 0000000000000001 RDI: 0000000000000000 RBP: ffff88811a17e620 R08: 0000000000000040 R09: 0000000000000000 R10: ffff88811a5c3618 R11: 0000000de85d51bd R12: ffff88811a17e600 R13: ffff88810d6f0a00 R14: 0000000000000000 R15: ffff8881034bda80 FS: 00007f27bdf89180(0000) GS:ffff88852c880000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000010 CR3: 000000010f159005 CR4: 0000000000372eb0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? __die+0x20/0x60 ? page_fault_oops+0x150/0x3e0 ? exc_page_fault+0x74/0x130 ? asm_exc_page_fault+0x22/0x30 ? mlx5_devcom_comp_set_ready+0x5/0x40 [mlx5_core] mlx5e_devcom_event_mpv+0x42/0x60 [mlx5_core] mlx5_devcom_send_event+0x8c/0x170 [mlx5_core] blocking_event+0x17b/0x230 [mlx5_core] notifier_call_chain+0x35/0xa0 blocking_notifier_call_chain+0x3d/0x60 mlx5_blocking_notifier_call_chain+0x22/0x30 [mlx5_core] mlx5_core_mp_event_replay+0x12/0x20 [mlx5_core] mlx5_ib_bind_slave_port+0x228/0x2c0 [mlx5_ib] mlx5_ib_stage_init_init+0x664/0x9d0 [mlx5_ib] ? idr_alloc_cyclic+0x50/0xb0 ? __kmalloc_cache_noprof+0x167/0x340 ? __kmalloc_noprof+0x1a7/0x430 __mlx5_ib_add+0x34/0xd0 [mlx5_ib] mlx5r_probe+0xe9/0x310 [mlx5_ib] ? kernfs_add_one+0x107/0x150 ? __mlx5_ib_add+0xd0/0xd0 [mlx5_ib] auxiliary_bus_probe+0x3e/0x90	N/A	More Details

	really_probe+0xc5/0x3a0 ? driver_probe_device+0x90/0x90 __driver_probe_device+0x80/0x160 driver_probe_device+0x1e/0x90 __device_attach_driver+0x7d/0x100 bus_for_each_drv+0x80/0xd0 __device_attach+0xbc/0x1f0 bus_probe_device+0x86/0xa0 device_add+0x62d/0x830 __auxiliary_device_add+0x3b/0xa0 ? auxiliary_device_init+0x41/0x90 add_adev+0xd1/0x150 [mlx5_core] mlx5_rescan_drivers_locked+0x21c/0x300 [mlx5_core] esw_mode_change+0x6c/0xc0 [mlx5_core] mlx5_devlink_eswitch_mode_set+0x21e/0x640 [mlx5_core] devlink_nl_eswitch_set_doit+0x60/0xe0 genl_family_rcv_msg_doit+0xd0/0x120 genl_rcv_msg+0x180/0x2b0 ? devlink_get_from_attrs_lock+0x170/0x170 ? devlink_nl_eswitch_get_doit+0x290/0x290 ? devlink_nl_pre_doit_port_optional+0x50/0x50 ? genl_family_rcv_msg_dumpit+0xf0/0xf0 netlink_rcv_skb+0x54/0x100 genl_rcv+0x24/0x40 netlink_unicast+0x1fc/0x2d0 netlink_sendmsg+0x1e4/0x410 __sock_sendmsg+0x38/0x60 ? sockfd_lookup_light+0x12/0x60 __sys_sendto+0x105/0x160 ? __sys_recvmsg+0x4e/0x90 __x64_sys_sendto+0x20/0x30 do_syscall_64+0x4c/0x100 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f27bc91b13a Code: bb 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 8b 05 fa 96 2c 00 45 89 c9 4c 63 d1 48 63 ff 85 c0 75 15 b8 2c 00 00 00 0f 05 <48> 3d 00 f0 ff ff ---truncated---		
CVE-2025-66622	matrix-sdk-base is the base component to build a Matrix client library. Versions 0.14.1 and prior are unable to handle responses that include custom m.room.join_rules values due to a serialization bug. This can be exploited to cause a denial-of-service condition, if a user is invited to a room with non-standard join rules, the crate's sync process will stall, preventing further processing for all rooms. This is fixed in version 0.16.0.	N/A	More Details
CVE-2025-66568	The ruby-saml library implements the client side of an SAML authorization. Versions up to and including 1.12.4, are vulnerable to authentication bypass through the libxml2 canonicalization process used by Nokogiri for document transformation, which allows an attacker to execute a Signature Wrapping attack. When libxml2's canonicalization is invoked on an invalid XML input, it may return an empty string rather than a canonicalized node. ruby-saml then proceeds to compute the DigestValue over this empty string, treating it as if canonicalization succeeded. This issue is fixed in version 1.18.0.	N/A	More Details
CVE-2025-67487	Static Web Server (SWS) is a production-ready web server suitable for static web files or assets. Versions 2.40.0 and below contain symbolic links (symlinks) which can be used to access files or directories outside the intended web root folder. SWS generally does not prevent symlinks from escaping the web server's root directory. Therefore, if a malicious actor gains access to the web server's root directory, they could create symlinks to access other files outside the designated web root folder either by URL or via the directory listing. This issue is fixed in version 2.40.1.	N/A	More Details
CVE-2025-66567	The ruby-saml library is for implementing the client side of a SAML authorization. ruby-saml versions up to and including 1.12.4 contain an authentication bypass vulnerability due to an incomplete fix for CVE-2025-25292. ReXML and Nokogiri parse XML differently, generating entirely different document structures from the same input. This allows an attacker to execute a Signature Wrapping attack. This issue is fixed in version 1.18.0.	N/A	More Details
CVE-2025-66565	Fiber Utils is a collection of common functions created for Fiber. In versions 2.0.0-rc.3 and below, when the system's cryptographic random number generator (crypto/rand) fails, both functions silently fall back to returning predictable UUID values, including the zero UUID "00000000-0000-0000-0000-000000000000". The vulnerability occurs through two related but distinct failure paths, both ultimately caused by crypto/rand.Read() failures, compromising the security of all Fiber applications using these functions for security-critical operations. This issue is fixed in version 2.0.0-rc.4.	N/A	More Details
CVE-2025-66534	Missing Authorization vulnerability in Elated-Themes The Aisle theaisle allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Aisle: from n/a through <= 2.9.	N/A	More Details
CVE-2025-40239	In the Linux kernel, the following vulnerability has been resolved: net: phy: micrel: always set shared->phydev for LAN8814 Currently, during the LAN8814 PTP probe shared->phydev is only set if PTP clock gets actually set, otherwise the function will return before setting it. This is an issue as shared->phydev is unconditionally being used when IRQ is being handled, especially in lan8814_gpio_process_cap and since it was not set it will cause a NULL pointer exception and crash the kernel. So, simply always set shared->phydev to avoid the NULL pointer exception.	N/A	More Details
CVE-2025-66532	Missing Authorization vulnerability in Mikado-Themes Powerlift powerlift allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Powerlift: from n/a through < 3.2.1.	N/A	More Details
CVE-2025-66531	Cross-Site Request Forgery (CSRF) vulnerability in Dimitri Grassi Salon booking system salon-booking-system allows Cross Site Request Forgery.This issue affects Salon booking system: from n/a through <= 10.30.3.	N/A	More Details
CVE-2025-66530	Missing Authorization vulnerability in Webba Appointment Booking Webba Booking webba-booking-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Webba Booking: from n/a through <= 6.2.1.	N/A	More Details
CVE-2025-66529	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Chartify chart-builder allows Cross Site Request Forgery.This issue affects Chartify: from n/a through <= 3.6.3.	N/A	More Details
CVE-2025-66528	Missing Authorization vulnerability in VillaTheme Thank You Page Customizer for WooCommerce woo-thank-you-page-customizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Thank You Page Customizer for WooCommerce: from n/a through <= 1.1.8.	N/A	More Details
CVE-2025-66527	Missing Authorization vulnerability in VanKarWai Lobo lobo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Lobo: from n/a through <= 2.8.6.	N/A	More Details
CVE-2025-65288	A buffer overflow in the Mercury MR816v2 (081C3114 4.8.7 Build 110427 Rel 36550n) occurs when the device accepts and stores excessively long hostnames from LAN hosts without proper length validation. The affected code performs unchecked copies/concatenations into fixed-size buffers. A crafted long hostname can overflow the buffer, cause a crash (DoS) and potentially enabling remote code execution.	N/A	More Details
CVE-2025-66525	Missing Authorization vulnerability in Elastic Email Elastic Email Sender elastic-email-sender allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Elastic Email Sender: from n/a through <= 1.2.20.	N/A	More Details
CVE-2025-40240	In the Linux kernel, the following vulnerability has been resolved: sctp: avoid NULL dereference when chunk data buffer is missing chunk->skb pointer is dereferenced in the if-block where it's supposed to be NULL only. chunk->skb can only be NULL if chunk->head_skb is not. Check for frag_list instead and do it just before replacing chunk->skb. We're sure that otherwise chunk->skb is non-NULL because of outer	N/A	More Details

	if() condition.		
CVE-2025-67474	Missing Authorization vulnerability in Ultimate Member ForumWP forumwp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ForumWP: from n/a through <= 2.1.4.	N/A	More Details
CVE-2025-67515	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Wilmër wilmer allows PHP Local File Inclusion.This issue affects Wilmër: from n/a through < 3.5.	N/A	More Details
CVE-2025-65594	OpenSIS 9.2 and below is vulnerable to Incorrect Access Control in Student.php, which allows an authenticated low-privilege user to perform unauthorized database write operations relating to the data of other users.	N/A	More Details
CVE-2025-67531	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in trippleS Turitor turitor allows PHP Local File Inclusion.This issue affects Turitor: from n/a through < 1.5.3.	N/A	More Details
CVE-2025-40229	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: fix potential memory leak by cleaning ops_filter in damon_destroy_scheme Currently, damon_destroy_scheme() only cleans up the filter list but leaves ops_filter untouched, which could lead to memory leaks when a scheme is destroyed. This patch ensures both filter and ops_filter are properly freed in damon_destroy_scheme(), preventing potential memory leaks.	N/A	More Details
CVE-2025-11531	HP System Event Utility and Omen Gaming Hub might allow execution of certain files outside of their restricted paths. This potential vulnerability was remediated with HP System Event Utility version 3.2.12 and Omen Gaming Hub version 1101.2511.101.0.	N/A	More Details
CVE-2025-40230	In the Linux kernel, the following vulnerability has been resolved: mm: prevent poison consumption when splitting THP When performing memory error injection on a THP (Transparent Huge Page) mapped to userspace on an x86 server, the kernel panics with the following trace. The expected behavior is to terminate the affected process instead of panicking the kernel, as the x86 Machine Check code can recover from an in-userspace #MC. mce: [Hardware Error]: CPU 0: Machine Check Exception: f Bank 3: bd80000000070134 mce: [Hardware Error]: RIP 10:<ffffffff8372f8bc> {memchr_inv+0x4c/0xf0} mce: [Hardware Error]: TSC afff7bbff88a ADDR 1d301b000 MISC 80 PPIN 1e741e77539027db mce: [Hardware Error]: PROCESSOR 0:d06d0 TIME 1758093249 SOCKET 0 APIC 0 microcode 80000320 mce: [Hardware Error]: Run the above through 'mcelog --ascii' mce: [Hardware Error]: Machine check: Data load in unrecoverable area of kernel Kernel panic - not syncing: Fatal local machine check The root cause of this panic is that handling a memory failure triggered by an in-userspace #MC necessitates splitting the THP. The splitting process employs a mechanism, implemented in try_to_map_unused_to_zeropage(), which reads the pages in the THP to identify zero-filled pages. However, reading the pages in the THP results in a second in-kernel #MC, occurring before the initial memory_failure() completes, ultimately leading to a kernel panic. See the kernel panic call trace on the two #MCs. First Machine Check occurs // [1] memory_failure() // [2] try_to_split_thp_page() split_huge_page() split_huge_page_to_list_to_order() __folio_split() // [3] remap_page() remove_migration_ptes() remove_migration_pte() try_to_map_unused_to_zeropage() // [4] memchr_inv() // [5] Second Machine Check occurs // [6] Kernel panic [1] Triggered by accessing a hardware-poisoned THP in userspace, which is typically recoverable by terminating the affected process. [2] Call folio_set_has_hwpoisoned() before try_to_split_thp_page(). [3] Pass the RMP_USE_SHARED_ZEROPAGE remap flag to remap_page(). [4] Try to map the unused THP to zeropage. [5] Re-access pages in the hw-poisoned THP in the kernel. [6] Triggered in-kernel, leading to a panic kernel. In Step[2], memory_failure() sets the poisoned flag on the page in the THP by TestSetPageHWPoison() before calling try_to_split_thp_page(). As suggested by David Hildenbrand, fix this panic by not accessing to the poisoned page in the THP during zeropage identification, while continuing to scan unaffected pages in the THP for possible zeropage mapping. This prevents a second in-kernel #MC that would cause kernel panic in Step[4]. Thanks to Andrew Zaborowski for his initial work on fixing this issue.	N/A	More Details
CVE-2025-40231	In the Linux kernel, the following vulnerability has been resolved: vsock: fix lock inversion in vsock_assign_transport() Syzbot reported a potential lock inversion deadlock between vsock_register_mutex and sk_lock-AF_VSOCK when vsock_linger() is called. The issue was introduced by commit 687aa0c5581b ("vsock: Fix transport_* TOCTOU") which added vsock_register_mutex locking in vsock_assign_transport() around the transport->release() call, that can call vsock_linger(). vsock_assign_transport() can be called with sk_lock held. vsock_linger() calls sk_wait_event() that temporarily releases and re-acquires sk_lock. During this window, if another thread hold vsock_register_mutex while trying to acquire sk_lock, a circular dependency is created. Fix this by releasing vsock_register_mutex before calling transport->release() and vsock_deassign_transport(). This is safe because we don't need to hold vsock_register_mutex while releasing the old transport, and we ensure the new transport won't disappear by obtaining a module reference first via try_module_get().	N/A	More Details
CVE-2025-40232	In the Linux kernel, the following vulnerability has been resolved: rv: Fully convert enabled_monitors to use list_head as iterator The callbacks in enabled_monitors_seq_ops are inconsistent. Some treat the iterator as struct rv_monitor *, while others treat the iterator as struct list_head *. This causes a wrong type cast and crashes the system as reported by Nathan. Convert everything to use struct list_head * as iterator. This also makes enabled_monitors consistent with available_monitors.	N/A	More Details
CVE-2025-40233	In the Linux kernel, the following vulnerability has been resolved: ocfs2: clear extent cache after moving/defragmenting extents The extent map cache can become stale when extents are moved or defragmented, causing subsequent operations to see outdated extent flags. This triggers a BUG_ON in ocfs2_refcount_cal_cow_clusters(). The problem occurs when: 1. copy_file_range() creates a reflinked extent with OCFS2_EXT_REFCOUNTED 2. ioctl(FITRIM) triggers ocfs2_move_extents() 3. __ocfs2_move_extents_range() reads and caches the extent (flags=0x2) 4. ocfs2_move_extent()/ocfs2_defrag_extent() calls __ocfs2_move_extent() which clears OCFS2_EXT_REFCOUNTED flag on disk (flags=0x0) 5. The extent map cache is not invalidated after the move 6. Later write() operations read stale cached flags (0x2) but disk has updated flags (0x0), causing a mismatch 7. BUG_ON(!(rec->e_flags & OCFS2_EXT_REFCOUNTED)) triggers Fix by clearing the extent map cache after each extent move/defrag operation in __ocfs2_move_extents_range(). This ensures subsequent operations read fresh extent data from disk.	N/A	More Details
CVE-2025-40234	In the Linux kernel, the following vulnerability has been resolved: platform/x86: alienware-wmi-wmax: Fix NULL pointer dereference in sleep handlers Devices without the AWCC interface don't initialize `awcc`. Add a check before dereferencing it in sleep handlers.	N/A	More Details
CVE-2025-40235	In the Linux kernel, the following vulnerability has been resolved: btrfs: directly free partially initialized fs_info in btrfs_check_leaked_roots() If fs_info->super_copy or fs_info->super_for_commit allocated failed in btrfs_get_tree_subvol(), then no need to call btrfs_free_fs_info(). Otherwise btrfs_check_leaked_roots() would access NULL pointer because fs_info->allocated_roots had not been initialised. syzkaller reported the following information: ------------[cut here]------------ BUG: unable to handle page fault for address: ffffffffffffffbb0 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 64c9067 P4D 64c9067 PUD 64cb067 PMD 0 Oops: Oops: 0000 [#1] SMP KASAN PTI CPU: 0 UID: 0 PID: 1402 Comm: syz.1.35 Not tainted 6.15.8 #4 PREEMPT(lazy) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), (...) RIP: 0010:arch_atomic_read arch/x86/include/asm/atomic.h:23 [inline] RIP: 0010:raw_atomic_read include/linux/atomic/atomic-arch-fallback.h:457 [inline] RIP: 0010:atomic_read include/linux/atomic/atomic-instrumented.h:33 [inline] RIP: 0010:refcount_read include/linux/refcount.h:170 [inline] RIP: 0010:btrfs_check_leaked_roots+0x18f/0x2c0	N/A	More Details

	fs/btrfs/disk-io.c:1230 [...] Call Trace: <TASK> btrfs_free_fs_info+0x310/0x410 fs/btrfs/disk-io.c:1280 btrfs_get_tree_subvol+0x592/0x6b0 fs/btrfs/super.c:2029 btrfs_get_tree+0x63/0x80 fs/btrfs/super.c:2097 vfs_get_tree+0x98/0x320 fs/super.c:1759 do_new_mount+0x357/0x660 fs/namespace.c:3899 path_mount+0x716/0x19c0 fs/namespace.c:4226 do_mount fs/namespace.c:4239 [inline] __do_sys_mount fs/namespace.c:4450 [inline] __se_sys_mount fs/namespace.c:4427 [inline] __x64_sys_mount+0x28c/0x310 fs/namespace.c:4427 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x92/0x180 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f032eaffa8d [...]		
CVE-2025-40236	In the Linux kernel, the following vulnerability has been resolved: virtio-net: zero unused hash fields When GSO tunnel is negotiated virtio_net_hdr_tnl_from_skb() tries to initialize the tunnel metadata but forget to zero unused rxhash fields. This may leak information to another side. Fixing this by zeroing the unused hash fields.	N/A	More Details
CVE-2025-40237	In the Linux kernel, the following vulnerability has been resolved: fs/notify: call exportfs_encode_fid with s_umount Calling intotify_show_fdinfo() on fd watching an overlayfs inode, while the overlayfs is being unmounted, can lead to dereferencing NULL ptr. This issue was found by syzkaller. Race Condition Diagram: Thread 1 Thread 2 -------- -------- generic_shutdown_super() shrink_dcache_for_umount sb->s_root = NULL | | vfs_read() | inotify_fdinfo() | * inode get from mark * | show_mark_fhandle(m, inode) | exportfs_encode_fid(inode, ..) | ovl_encode_fh(inode, ..) | ovl_check_encode_origin(inode) | * deref i_sb->s_root * | | v fsnotify_sb_delete(sb) Which then leads to: [32.133461] Oops: general protection fault, probably for non-canonical address 0xdffffc0000000006: 0000 [#1] SMP DEBUG_PAGEALLOC KASAN NOPTI [32.134438] KASAN: null-ptr-deref in range [0x0000000000000030-0x0000000000000037] [32.135032] CPU: 1 UID: 0 PID: 4468 Comm: systemd-coredum Not tainted 6.17.0-rc6 #22 PREEMPT(none) <snip registers, unreliable trace> [32.143353] Call Trace: [32.143732] ovl_encode_fh+0xd5/0x170 [32.144031] exportfs_encode_inode_fh+0x12f/0x300 [32.144425] show_mark_fhandle+0xbe/0x1f0 [32.145805] inotify_fdinfo+0x226/0x2d0 [32.146442] inotify_show_fdinfo+0x1c5/0x350 [32.147168] seq_show+0x530/0x6f0 [32.147449] seq_read_iter+0x503/0x12a0 [32.148419] seq_read+0x31f/0x410 [32.150714] vfs_read+0x1f0/0x9e0 [32.152297] ksys_read+0x125/0x240 IOW ovl_check_encode_origin derefs inode->i_sb->s_root, after it was set to NULL in the unmount path. Fix it by protecting calling exportfs_encode_fid() from show_mark_fhandle() with s_umount lock. This form of fix was suggested by Amir in [1]. [1]: https://lore.kernel.org/all/CAOQ4uxhbDwhb+2Brs1UdkoF0a3NSdBAOQPNfEHjahrgoKJpLEw@mail.gmail.com/	N/A	More Details
CVE-2025-67534	Cross-Site Request Forgery (CSRF) vulnerability in Jacques Malgrange Rencontre rencontre allows Stored XSS.This issue affects Rencontre: from n/a through <= 3.13.7.	N/A	More Details
CVE-2025-67533	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Portfolio Post themify-portfolio-post allows Stored XSS.This issue affects Themify Portfolio Post: from n/a through <= 1.3.0.	N/A	More Details
CVE-2025-67532	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Hara hara allows PHP Local File Inclusion.This issue affects Hara: from n/a through <= 1.2.17.	N/A	More Details
CVE-2025-67530	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Besa besa allows PHP Local File Inclusion.This issue affects Besa: from n/a through <= 2.3.15.	N/A	More Details
CVE-2025-67516	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Agile Logix Store Locator WordPress agile-store-locator allows Blind SQL Injection.This issue affects Store Locator WordPress: from n/a through <= 1.6.2.	N/A	More Details
CVE-2025-67529	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Opal_WP Fashion fashion2 allows PHP Local File Inclusion.This issue affects Fashion: from n/a through < 5.3.0.	N/A	More Details
CVE-2025-39665	User enumeration in Nagvis' Checkmk MultisiteAuth before version 1.9.48 allows an unauthenticated attacker to enumerate Checkmk usernames.	N/A	More Details
CVE-2025-67527	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in trippleS Digiqole digiqole allows PHP Local File Inclusion.This issue affects Digiqole: from n/a through < 2.2.7.	N/A	More Details
CVE-2025-67526	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThimPress Sailing sailing allows PHP Local File Inclusion.This issue affects Sailing: from n/a through < 4.4.6.	N/A	More Details
CVE-2025-67525	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Opal_WP ekommart ekommart allows PHP Local File Inclusion.This issue affects ekommart: from n/a through < 4.3.1.	N/A	More Details
CVE-2025-67524	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in NooTheme Jobmonster Elementor Addon jobmonster-addon allows PHP Local File Inclusion.This issue affects Jobmonster Elementor Addon: from n/a through <= 1.1.4.	N/A	More Details
CVE-2025-67523	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in trippleS Exhibz exhibz allows PHP Local File Inclusion.This issue affects Exhibz: from n/a through <= 3.0.9.	N/A	More Details
CVE-2025-67522	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in NooTheme Jobmonster noo-jobmonster allows PHP Local File Inclusion.This issue affects Jobmonster: from n/a through <= 4.8.2.	N/A	More Details
CVE-2025-67521	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Select Core select-core allows PHP Local File Inclusion.This issue affects Select Core: from n/a through < 2.6.	N/A	More Details
CVE-2025-67520	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tiny Solutions Media Library Tools media-library-tools allows SQL Injection.This issue affects Media Library Tools: from n/a through <= 1.6.15.	N/A	More Details

CVE-2025-67519	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shahjahan Jewel Ninja Tables ninja-tables allows SQL Injection.This issue affects Ninja Tables: from n/a through <= 5.2.3.	N/A	More Details
CVE-2025-67518	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup Accordion Slider PRO accordion_slider_pro allows Blind SQL Injection.This issue affects Accordion Slider PRO: from n/a through <= 1.2.	N/A	More Details
CVE-2025-67517	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in artplacer ArtPlacer Widget artplacer-widget allows Blind SQL Injection.This issue affects ArtPlacer Widget: from n/a through <= 2.22.9.2.	N/A	More Details
CVE-2025-62090	Missing Authorization vulnerability in Jegstudio Gutenverse News – Advanced News Magazine Blog Gutenberg Blocks Addons gutenverse-news allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gutenverse News – Advanced News Magazine Blog Gutenberg Blocks Addons: from n/a through <= 3.0.2.	N/A	More Details
CVE-2025-10655	SQL Injection in Frappe HelpDesk in the dashboard get_dashboard_data due to unsafe concatenation of user-controlled parameters into dynamic SQL statements.This issue affects Frappe HelpDesk: 1.14.0.	N/A	More Details
CVE-2025-62085	Missing Authorization vulnerability in berthaai BERTHA AI bertha-ai-free allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BERTHA AI: from n/a through <= 1.13.	N/A	More Details
CVE-2022-50626	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb: fix memory leak in dvb_usb_adapter_init() Syzbot reports a memory leak in "dvb_usb_adapter_init()". The leak is due to not accounting for and freeing current iteration's adapter->priv in case of an error. Currently if an error occurs, it will exit before incrementing "num_adapters_initalized", which is used as a reference counter to free all adap->priv in "dvb_usb_adapter_exit()". There are multiple error paths that can exit from before incrementing the counter. Including the error handling paths for "dvb_usb_adapter_stream_init()", "dvb_usb_adapter_dvb_init()" and "dvb_usb_adapter_frontend_init()" within "dvb_usb_adapter_init()". This means that in case of an error in any of these functions the current iteration is not accounted for and the current iteration's adap->priv is not freed. Fix this by freeing the current iteration's adap->priv in the "stream_init_err:" label in the error path. The rest of the (accounted for) adap->priv objects are freed in dvb_usb_adapter_exit() as expected using the num_adapters_initalized variable. Syzbot report: BUG: memory leak unreferenced object 0xffff8881172f1a00 (size 512): comm "kworker/0:2", pid 139, jiffies 4294994873 (age 10.960s) 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: [<ffffffff844af012>] dvb_usb_adapter_init drivers/media/usb/dvb-usb/dvb-usb-init.c:75 [inline] [<ffffffff844af012>] dvb_usb_init drivers/media/usb/dvb-usb/dvb-usb-init.c:184 [inline] [<ffffffff844af012>] dvb_usb_device_init.cold+0x4e5/0x79e drivers/media/usb/dvb-usb/dvb-usb-init.c:308 [<ffffffff830db21d>] dib0700_probe+0x8d/0x1b0 drivers/media/usb/dvb-usb/dib0700_core.c:883 [<ffffffff82d3fdc7>] usb_probe_interface+0x177/0x370 drivers/usb/core/driver.c:396 [<ffffffff8274ab37>] call_driver_probe drivers/base/dd.c:542 [inline] [<ffffffff8274ab37>] really_probe.part.0+0xe7/0x310 drivers/base/dd.c:621 [<ffffffff8274ae6c>] really_probe drivers/base/dd.c:583 [inline] [<ffffffff8274ae6c>] __driver_probe_device+0x10c/0x1e0 drivers/base/dd.c:752 [<ffffffff8274af6a>] driver_probe_device+0x2a/0x120 drivers/base/dd.c:782 [<ffffffff8274b786>] __device_attach_driver+0xf6/0x140 drivers/base/dd.c:899 [<ffffffff82747c87>] bus_for_each_drv+0xb7/0x100 drivers/base/bus.c:427 [<ffffffff8274b352>] __device_attach+0x122/0x260 drivers/base/dd.c:970 [<ffffffff827498f6>] bus_probe_device+0xc6/0xe0 drivers/base/bus.c:487 [<ffffffff82745cdb>] device_add+0x5fb/0xdf0 drivers/base/core.c:3405 [<ffffffff82d3d202>] usb_set_configuration+0x8f2/0xb80 drivers/usb/core/message.c:2170 [<ffffffff82d4dbfc>] usb_generic_driver_probe+0x8c/0xc0 drivers/usb/core/generic.c:238 [<ffffffff82d3f49c>] usb_probe_device+0x5c/0x140 drivers/usb/core/driver.c:293 [<ffffffff8274ab37>] call_driver_probe drivers/base/dd.c:542 [inline] [<ffffffff8274ab37>] really_probe.part.0+0xe7/0x310 drivers/base/dd.c:621 [<ffffffff8274ae6c>] really_probe drivers/base/dd.c:583 [inline] [<ffffffff8274ae6c>] __driver_probe_device+0x10c/0x1e0 drivers/base/dd.c:752	N/A	More Details
CVE-2023-53763	In the Linux kernel, the following vulnerability has been resolved: Revert "f2fs: fix to do sanity check on extent cache correctly" syzbot reports a f2fs bug as below: UBSAN: array-index-out-of-bounds in fs/f2fs/f2fs.h:3275:19 index 1409 is out of range for type '__le32[923]' (aka 'unsigned int[923]') Call Trace: __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1e7/0x2d0 lib/dump_stack.c:106 ubsan_epilogue lib/ubsan.c:217 [inline] __ubsan_handle_out_of_bounds+0x11c/0x150 lib/ubsan.c:348 inline_data_addr fs/f2fs/f2fs.h:3275 [inline] __recover_inline_status fs/f2fs/inode.c:113 [inline] do_read_inode fs/f2fs/inode.c:480 [inline] f2fs_iget+0x4730/0x48b0 fs/f2fs/inode.c:604 f2fs_fill_super+0x640e/0x80c0 fs/f2fs/super.c:4601 mount_bdev+0x276/0x3b0 fs/super.c:1391 legacy_get_tree+0xef/0x190 fs/fs_context.c:611 vfs_get_tree+0x8c/0x270 fs/super.c:1519 do_new_mount+0x28f/0xae0 fs/namespace.c:3335 do_mount fs/namespace.c:3675 [inline] __do_sys_mount fs/namespace.c:3884 [inline] __se_sys_mount+0x2d9/0x3c0 fs/namespace.c:3861 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 issue was bisected to: commit d48a7b3a72f121655d95b5157c32c7d555e44c05 Author: Chao Yu <chao@kernel.org> Date: Mon Jan 9 03:49:20 2023 +0000 f2fs: fix to do sanity check on extent cache correctly The root cause is we applied both v1 and v2 of the patch, v2 is the right fix, so it needs to revert v1 in order to fix reported issue. v1: commit d48a7b3a72f1 ("f2fs: fix to do sanity check on extent cache correctly") https://lore.kernel.org/lkml/20230109034920.492914-1-chao@kernel.org/ v2: commit 269d11948100 ("f2fs: fix to do sanity check on extent cache correctly") https://lore.kernel.org/lkml/20230207134808.1827869-1-chao@kernel.org/	N/A	More Details
CVE-2023-53764	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Handle lock during peer_id find ath12k_peer_find_by_id() requires that the caller hold the ab->base_lock. Currently the WBM error path does not hold the lock and calling that function, leads to the following lockdep_assert()in QCN9274: [105162.160893] ------------[cut here]------------ [105162.160916] WARNING: CPU: 3 PID: 0 at drivers/net/wireless/ath/ath12k/peer.c:71 ath12k_peer_find_by_id+0x52/0x60 [ath12k] [105162.160933] Modules linked in: ath12k(O) qrtr_mhi qrtr mac80211 cfg80211 mhi qmi_helpers libarc4 nvme nvme_core [last unloaded: ath12k(O)] [105162.160967] CPU: 3 PID: 0 Comm: swapper/3 Tainted: G W O 6.1.0-rc2+ #3 [105162.160972] Hardware name: Intel(R) Client Systems NUC8i7HVK/NUC8i7HVB, BIOS HNKBLi70.86A.0056.2019.0506.1527 05/06/2019 [105162.160977] RIP: 0010:ath12k_peer_find_by_id+0x52/0x60 [ath12k] [105162.160990] Code: 07 eb 0f 39 68 24 74 0a 48 8b 00 48 39 f8 75 f3 31 c0 5b 5d c3 48 8d bf b0 f2 00 00 be ff ff ff ff e8 22 20 c4 e2 85 c0 75 bf <0f> 0b eb bb 66 2e 0f 1f 84 00 00 00 00 00 41 54 4c 8d a7 98 f2 00 [105162.160996] RSP: 0018:ffffa223001acc60 EFLAGS: 00010246 [105162.161003] RAX: 0000000000000000 RBX: ffff9f0573940000 RCX: 0000000000000000 [105162.161008] RDX: 0000000000000001 RSI: ffffffffa3951c8e RDI: ffffffffa39a96d7 [105162.161013] RBP: 000000000000000a R08: 0000000000000000 R09: 0000000000000000 [105162.161017] R10: ffffa223001acb40 R11: ffffffffa3d57c60 R12: ffff9f057394f2e0 [105162.161022] R13: ffff9f0573940000 R14: ffff9f04ecd659c0 R15: ffff9f04d5a9b040 [105162.161026] FS: 0000000000000000(0000) GS:ffff9f0575600000(0000) knlGS:0000000000000000 [105162.161031] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [105162.161036] CR2: 00001d5c8277a008 CR3: 00000001e6224006 CR4: 00000000003706e0 [105162.161041] Call Trace: [105162.161046] <IRQ> [105162.161051] ath12k_dp_rx_process_wbm_err+0x6da/0xaf0 [ath12k] [105162.161072] ? ath12k_dp_rx_process_err+0x80e/0x15a0 [ath12k] [105162.161084] ? __lock_acquire+0x4ca/0x1a60 [105162.161104] ath12k_dp_service_srng+0x263/0x310 [ath12k] [105162.161120] ath12k_pci_ext_grp_napi_poll+0x1c/0x70 [ath12k] [105162.161133] __napi_poll+0x22/0x260 [105162.161141] net_rx_action+0x2f8/0x380 [105162.161153] __do_softirq+0xd0/0x4c9 [105162.161162] irq_exit_rcu+0x88/0xe0 [105162.161169] common_interrupt+0xa5/0xc0 [105162.161174] </IRQ> [105162.161179] <TASK>	N/A	More Details

	[105162.161184] asm_common_interrupt+0x22/0x40 Handle spin lock/unlock in WBM error path to hold the necessary lock expected by ath12k_peer_find_by_id(). Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.0-03171-QCAHKSWPL_SILICONZ-1		
CVE-2023-53765	In the Linux kernel, the following vulnerability has been resolved: dm cache: free background tracker's queued work in btracker_destroy Otherwise the kernel can BUG with: [2245.426978] ========== [2245.435155] BUG bt_work (Tainted: G B W): Objects remaining in bt_work on __kmem_cache_shutdown() [2245.445233] ---------- [2245.445233] [2245.454879] Slab 0x00000000b0ce2b30 objects=64 used=2 fp=0x000000000a3c6a4e flags=0x17ffffc0000200(slab|node=0|zone=2|lastcpupid=0x1fffff) [2245.467300] CPU: 7 PID: 10805 Comm: lvm Kdump: loaded Tainted: G B W 6.0.0-rc2 #19 [2245.476078] Hardware name: Dell Inc. PowerEdge R7525/0590KW, BIOS 2.5.6 10/06/2021 [2245.483646] Call Trace: [2245.486100] <TASK> [2245.488206] dump_stack_lvl+0x34/0x48 [2245.491878] slab_err+0x95/0xcd [2245.495028] __kmem_cache_shutdown.cold+0x31/0x136 [2245.499821] kmem_cache_destroy+0x49/0x130 [2245.503928] btracker_destroy+0x12/0x20 [dm_cache] [2245.508728] smq_destroy+0x15/0x60 [dm_cache_smq] [2245.513435] dm_cache_policy_destroy+0x12/0x20 [dm_cache] [2245.518834] destroy+0xc0/0x110 [dm_cache] [2245.522933] dm_table_destroy+0x5c/0x120 [dm_mod] [2245.527649] __dm_destroy+0x10e/0x1c0 [dm_mod] [2245.532102] dev_remove+0x117/0x190 [dm_mod] [2245.536384] ctl_ioctl+0x1a2/0x290 [dm_mod] [2245.540579] dm_ctl_ioctl+0xa/0x20 [dm_mod] [2245.544773] __x64_sys_ioctl+0x8a/0xc0 [2245.548524] do_syscall_64+0x5c/0x90 [2245.552104] ? syscall_exit_to_user_mode+0x12/0x30 [2245.556897] ? do_syscall_64+0x69/0x90 [2245.560648] ? do_syscall_64+0x69/0x90 [2245.564394] entry_SYSCALL_64_after_hwframe+0x63/0xcd [2245.569447] RIP: 0033:0x7fe52583ec6b ... [2245.646771] ----------[cut here]---------- [2245.651395] kmem_cache_destroy bt_work: Slab cache still has objects when called from btracker_destroy+0x12/0x20 [dm_cache] [2245.651408] WARNING: CPU: 7 PID: 10805 at mm/slab_common.c:478 kmem_cache_destroy+0x128/0x130 Found using: lvm2-testsuite --only "cache-single-split.sh" Ben bisected and found that commit 0495e337b703 ("mm/slab_common: Deleting kobject in kmem_cache_destroy() without holding slab_mutex/cpu_hotplug_lock") first exposed dm-cache's incomplete cleanup of its background tracker work objects.	N/A	More Details
CVE-2023-53766	In the Linux kernel, the following vulnerability has been resolved: FS: JFS: Check for read-only mounted filesystem in txBegin This patch adds a check for read-only mounted filesystem in txBegin before starting a transaction potentially saving from NULL pointer deref.	N/A	More Details
CVE-2023-53767	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix memory leak in ath12k_qmi_driver_event_work() Currently the buffer pointed by event is not freed in case ATH12K_FLAG_UNREGISTERING bit is set, this causes memory leak. Add a goto skip instead of return, to ensure event and all the list entries are freed properly. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.0.1-00029-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2023-53768	In the Linux kernel, the following vulnerability has been resolved: regmap-irq: Fix out-of-bounds access when allocating config buffers When allocating the 2D array for handling IRQ type registers in regmap_add_irq_chip_fwnode(), the intent is to allocate a matrix with num_config_bases rows and num_config_regs columns. This is currently handled by allocating a buffer to hold a pointer for each row (i.e. num_config_bases). After that, the logic attempts to allocate the memory required to hold the register configuration for each row. However, instead of doing this allocation for each row (i.e. num_config_bases allocations), the logic erroneously does this allocation num_config_regs number of times. This scenario can lead to out-of-bounds accesses when num_config_regs is greater than num_config_bases. Fix this by updating the terminating condition of the loop that allocates the memory for holding the register configuration to allocate memory only for each row in the matrix. Amit Pundir reported a crash that was occurring on his db845c device due to memory corruption (see "Closes" tag for Amit's report). The KASAN report below helped narrow it down to this issue: [14.033877][T1] ========== [14.042507][T1] BUG: KASAN: invalid-access in regmap_add_irq_chip_fwnode+0x594/0x1364 [14.050796][T1] Write of size 8 at addr 06ffff8081021850 by task init/1 [14.242004][T1] The buggy address belongs to the object at ffffff8081021850 [14.242004][T1] which belongs to the cache kmalloc-8 of size 8 [14.255669][T1] The buggy address is located 0 bytes inside of [14.255669][T1] 8-byte region [ffffff8081021850, ffffff8081021858)	N/A	More Details
CVE-2023-53769	In the Linux kernel, the following vulnerability has been resolved: virt/coco/sev-guest: Double-buffer messages The encryption algorithms read and write directly to shared unencrypted memory, which may leak information as well as permit the host to tamper with the message integrity. Instead, copy whole messages in or out as needed before doing any computation on them.	N/A	More Details
CVE-2025-66418	urllib3 is a user-friendly HTTP client library for Python. Starting in version 1.24 and prior to 2.6.0, the number of links in the decompression chain was unbounded allowing a malicious server to insert a virtually unlimited number of compression steps leading to high CPU usage and massive memory allocation for the decompressed data. This vulnerability is fixed in 2.6.0.	N/A	More Details
CVE-2025-6966	NULL pointer dereference in TagSection.keys() in python-apt on APT-based Linux systems allows a local attacker to cause a denial of service (process crash) via a crafted deb822 file with a malformed non-UTF-8 key.	N/A	More Details
CVE-2025-14262	A wrong permission check in KNIME Business Hub before version 1.17.0 allowed an authenticated user to save jobs of other users as if there were saved by the job owner. The attacker must have permissions to access the jobs but then they were saved into the catalog service using the wrong owner permissions. Therefore it may have been possible to save into spaces where the attacker does not have write permissions. There is no workaround.	N/A	More Details
CVE-2025-66461	FULLBACK Manager Pro provided by GS Yuasa International Ltd. registers two Windows services with unquoted file paths. A user may execute arbitrary code with SYSTEM privilege if he/she has the write permission on the path to the directory where the affected product is installed.	N/A	More Details
CVE-2025-42615	In affected versions, vulnerability-lookup did not track or limit failed One-Time Password (OTP) attempts during Two-Factor Authentication (2FA) verification. An attacker who already knew or guessed a valid username and password could submit an arbitrary number of OTP codes without causing the account to be locked or generating any specific alert for administrators. This lack of rate-limiting and lockout on OTP failures significantly lowers the cost of online brute-force attacks against 2FA codes and increases the risk of successful account takeover, especially if OTP entropy is reduced (e.g. short numeric codes, user reuse, or predictable tokens). Additionally, administrators had no direct visibility into accounts experiencing repeated 2FA failures, making targeted attacks harder to detect and investigate. The patch introduces a persistent failed_otp_attempts counter on user accounts, locks the user after 5 invalid OTP submissions, resets the counter on successful verification, and surfaces failed 2FA attempts in the admin user list. This enforces an account lockout policy for OTP brute-force attempts and improves monitoring capabilities for suspicious 2FA activity.This issue affects Vulnerability-Lookup: before 2.18.0.	N/A	More Details
CVE-2025-42616	Some endpoints in vulnerability-lookup that modified application state (e.g. changing database entries, user data, configurations, or other privileged actions) may have been accessible via HTTP GET requests without requiring a CSRF token. This flaw leaves the application vulnerable to Cross-Site Request Forgery (CSRF) attacks: an attacker who tricks a logged-in user into visiting a malicious website could cause the user's browser to issue GET requests that perform unintended state-changing operations in the context of their authenticated session. Because the server would treat these GET requests as valid (since no CSRF protection or POST method enforcement was in place), the attacker could exploit this to escalate privileges, change settings, or carry out other unauthorized actions without needing the user's	N/A	More Details

	explicit consent or awareness. The fix ensures that all state-changing endpoints now require HTTP POST requests and include a valid CSRF token. This enforces that state changes cannot be triggered by arbitrary cross-site GET requests. This issue affects Vulnerability-Lookup: before 2.18.0.		
CVE-2025-42620	In affected versions, vulnerability-lookup handled user-controlled content in comments and bundles in an unsafe way, which could lead to stored Cross-Site Scripting (XSS). On the backend, the related_vulnerabilities field of bundles accepted arbitrary strings without format validation or proper sanitization. On the frontend, comment and bundle descriptions were converted from Markdown to HTML and then injected directly into the DOM using string templates and innerHTML. This combination allowed an attacker who could create or edit comments or bundles to store crafted HTML/JavaScript payloads which would later be rendered and executed in the browser of any user visiting the affected profile page (user.html). This issue affects Vulnerability-Lookup: before 2.18.0.	N/A	More Details
CVE-2025-14271	Rejected reason: This CVE ID has been withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-66544	Rejected reason: Not used	N/A	More Details
CVE-2025-66543	Rejected reason: Not used	N/A	More Details
CVE-2025-66542	Rejected reason: Not used	N/A	More Details
CVE-2025-66541	Rejected reason: Not used	N/A	More Details
CVE-2025-66540	Rejected reason: Not used	N/A	More Details
CVE-2025-66539	Rejected reason: Not used	N/A	More Details
CVE-2023-53762	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: Fix UAF in hci_disconnect_all_sync Use-after-free can occur in hci_disconnect_all_sync if a connection is deleted by concurrent processing of a controller event. To prevent this the code now tries to iterate over the list backwards to ensure the links are cleanup before its parents, also it no longer relies on a cursor, instead it always uses the last element since hci_abort_conn_sync is guaranteed to call hci_conn_del. UAF crash log: == BUG: KASAN: slab-use-after-free in hci_set_powered_sync (net/bluetooth/hci_sync.c:5424) [bluetooth] Read of size 8 at addr ffff888009d9c000 by task kworker/u9:0/124 CPU: 0 PID: 124 Comm: kworker/u9:0 Tainted: G W 6.5.0-rc1+ #10 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.2-1.fc38 04/01/2014 Workqueue: hci0 hci_cmd_sync_work [bluetooth] Call Trace: <TASK> dump_stack_lvl+0x5b/0x90 print_report+0xcf/0x670 ? __virt_addr_valid+0xdd/0x160 ? hci_set_powered_sync+0x2c9/0x4a0 [bluetooth] kasan_report+0xa6/0xe0 ? hci_set_powered_sync+0x2c9/0x4a0 [bluetooth] ? __pfx_set_powered_sync+0x10/0x10 [bluetooth] hci_set_powered_sync+0x2c9/0x4a0 [bluetooth] ? __pfx_hci_set_powered_sync+0x10/0x10 [bluetooth] ? __pfx_lock_release+0x10/0x10 ? __pfx_set_powered_sync+0x10/0x10 [bluetooth] hci_cmd_sync_work+0x137/0x220 [bluetooth] process_one_work+0x526/0x9d0 ? __pfx_process_one_work+0x10/0x10 ? __pfx_do_raw_spin_lock+0x10/0x10 ? mark_held_locks+0x1a/0x90 worker_thread+0x92/0x630 ? __pfx_worker_thread+0x10/0x10 kthread+0x196/0x1e0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2c/0x50 </TASK> Allocated by task 1782: kasan_save_stack+0x33/0x60 kasan_set_track+0x25/0x30 __kasan_kmalloc+0x8f/0xa0 hci_conn_add+0xa5/0xa80 [bluetooth] hci_bind_cis+0x881/0x9b0 [bluetooth] iso_connect_cis+0x121/0x520 [bluetooth] iso_sock_connect+0x3f6/0x790 [bluetooth] __sys_connect+0x109/0x130 __x64_sys_connect+0x40/0x50 do_syscall_64+0x60/0x90 entry_SYSCALL_64_after_hwframe+0x6e/0xd8 Freed by task 695: kasan_save_stack+0x33/0x60 kasan_set_track+0x25/0x30 kasan_save_free_info+0x2b/0x50 __kasan_slab_free+0x10a/0x180 __kmem_cache_free+0x14d/0x2e0 device_release+0x5d/0xf0 kobject_put+0xdf/0x270 hci_disconn_complete_evt+0x274/0x3a0 [bluetooth] hci_event_packet+0x579/0x7e0 [bluetooth] hci_rx_work+0x287/0xaa0 [bluetooth] process_one_work+0x526/0x9d0 worker_thread+0x92/0x630 kthread+0x196/0x1e0 ret_from_fork+0x2c/0x50 ==	N/A	More Details
CVE-2023-53761	In the Linux kernel, the following vulnerability has been resolved: USB: usbtmc: Fix direction for 0-length ioctl control messages The syzbot fuzzer found a problem in the usbtmc driver: When a user submits an ioctl for a 0-length control transfer, the driver does not check that the direction is set to OUT: ------------[cut here]------------ usb 3-1: BOGUS control dir, pipe 80000b80 doesn't match bRequestType fd WARNING: CPU: 0 PID: 5100 at drivers/usb/core/urb.c:411 usb_submit_urb+0x14a7/0x1880 drivers/usb/core/urb.c:411 Modules linked in: CPU: 0 PID: 5100 Comm: syz-executor428 Not tainted 6.3.0-syzkaller-12049-g58390c8ce1bd #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/14/2023 RIP: 0010:usb_submit_urb+0x14a7/0x1880 drivers/usb/core/urb.c:411 Code: 7c 24 40 e8 1b 13 5c fb 48 8b 7c 24 40 e8 21 1d f0 fe 45 89 e8 44 89 f1 4c 89 e2 48 89 c6 48 c7 c7 e0 b5 fc 8a e8 19 c8 23 fb <0f> 0b e9 9f ee ff ff e8 ed 12 5c fb 0f b6 1d 12 8a 3c 08 31 ff 41 RSP: 0018:ffffc90003d2fb00 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffff8880789e9058 RCX: 0000000000000000 RDX: ffff888029593b80 RSI: ffffffff814c1447 RDI: 0000000000000001 RBP: ffff88801ea742f8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000001 R11: 0000000000000001 R12: ffff88802915e528 R13: 00000000000000fd R14: 0000000080000b80 R15: ffff8880222b3100 FS: 0000555556ca63c0(0000) GS:ffff8880b9800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f9ef4d18150 CR3: 0000000073e5b000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> usb_start_wait_urb+0x101/0x4b0 drivers/usb/core/message.c:58 usb_internal_control_msg drivers/usb/core/message.c:102 [inline] usb_control_msg+0x320/0x4a0 drivers/usb/core/message.c:153 usbtmc_ioctl_request drivers/usb/class/usbtmc.c:1954 [inline] usbtmc_ioctl+0x1b3d/0x2840 drivers/usb/class/usbtmc.c:2097 To fix this, we must override the direction in the bRequestType field of the control request structure when the length is 0.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: mcq: Fix &hwq->cq_lock deadlock issue When ufshcd_err_handler() is executed, CQ event interrupt can enter waiting for the same lock. This can happen in ufshcd_handle_mcq_cq_events() and also in ufs_mtk_mcq_intr(). The following warning message will be generated when &hwq->cq_lock is used in IRQ context with IRQ enabled. Use ufshcd_mcq_poll_cqe_lock() with spin_lock_irqsave instead of spin_lock to resolve the deadlock issue. [name:lockdep&]WARNING: inconsistent lock state [name:lockdep&]-------------------------------- [name:lockdep&]inconsistent {IN-HARDIRQ-W} -> {HARDIRQ-ON-W} usage. [name:lockdep&]kworker/u16:4/260 [HC0[0]:SC0[0]:HE1:SE1] takes: ffffff8028444600 (&hwq-		

CVE-2023-53760	>cq_lock){?.-.}-{2:2}, at: ufshcd_mcq_poll_cqe_lock+0x30/0xe0 [name:lockdep&]{IN-HARDIRQ-W} state was registered at: lock_acquire+0x17c/0x33c _raw_spin_lock+0x5c/0x7c ufshcd_mcq_poll_cqe_lock+0x30/0xe0 ufs_mtk_mcq_intr+0x60/0x1bc [ufs_mediatek_mod] __handle_irq_event_percpu+0x140/0x3ec handle_irq_event+0x50/0xd8 handle_fasteoi_irq+0x148/0x2b0 generic_handle_domain_irq+0x4c/0x6c gic_handle_irq+0x58/0x134 call_on_irq_stack+0x40/0x74 do_interrupt_handler+0x84/0xe4 el1_interrupt+0x3c/0x78 <snip> Possible unsafe locking scenario: CPU0 ---- lock(&hwq->cq_lock); <Interrupt> lock(&hwq->cq_lock); *** DEADLOCK *** 2 locks held by kworker/u16:4/260: [name:lockdep&] stack backtrace: CPU: 7 PID: 260 Comm: kworker/u16:4 Tainted: G S W OE 6.1.17-mainline-android14-2-g277223301adb #1 Workqueue: ufs_eh_wq_0 ufshcd_err_handler Call trace: dump_backtrace+0x10c/0x160 show_stack+0x20/0x30 dump_stack_lvl+0x98/0xd8 dump_stack+0x20/0x60 print_usage_bug+0x584/0x76c mark_lock_irq+0x488/0x510 mark_lock+0x1ec/0x25c __lock_acquire+0x4d8/0xffc lock_acquire+0x17c/0x33c _raw_spin_lock+0x5c/0x7c ufshcd_mcq_poll_cqe_lock+0x30/0xe0 ufshcd_poll+0x68/0x1b0 ufshcd_transfer_req_compl+0x9c/0xc8 ufshcd_err_handler+0x3bc/0xea0 process_one_work+0x2f4/0x7e8 worker_thread+0x234/0x450 kthread+0x110/0x134 ret_from_fork+0x10/0x20	N/A	More Details
CVE-2023-53748	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: Fix potential array out-of-bounds in decoder queue_setup variable *nplanes is provided by user via system call argument. The possible value of q_data->fmt->num_planes is 1-3, while the value of *nplanes can be 1-8. The array access by index i can cause array out-of-bounds. Fix this bug by checking *nplanes against the array size.	N/A	More Details
CVE-2022-50628	In the Linux kernel, the following vulnerability has been resolved: drm/gud: Fix UBSAN warning UBSAN complains about invalid value for bool: [101.165172] [drm] Initialized gud 1.0.0 20200422 for 2-3.2:1.0 on minor 1 [101.213360] gud 2-3.2:1.0: [drm] fb1: guddrmfb frame buffer device [101.213426] usbcore: registered new interface driver gud [101.989431] == [101.989441] UBSAN: invalid-load in linux/include/linux/iosys-map.h:253:9 [101.989447] load of value 121 is not a valid value for type '_Bool' [101.989451] CPU: 1 PID: 455 Comm: kworker/1:6 Not tainted 5.18.0-rc5-gud-5.18-rc5 #3 [101.989456] Hardware name: Hewlett-Packard HP EliteBook 820 G1/1991, BIOS L71 Ver. 01.44 04/12/2018 [101.989459] Workqueue: events_long gud_flush_work [gud] [101.989471] Call Trace: [101.989474] <TASK> [101.989479] dump_stack_lvl+0x49/0x5f [101.989488] dump_stack+0x10/0x12 [101.989493] ubsan_epilogue+0x9/0x3b [101.989498] __ubsan_handle_load_invalid_value.cold+0x44/0x49 [101.989504] dma_buf_vmap.cold+0x38/0x3d [101.989511] ? find_busiest_group+0x48/0x300 [101.989520] drm_gem_shmem_vmap+0x76/0x1b0 [drm_shmem_helper] [101.989528] drm_gem_shmem_object_vmap+0x9/0xb [drm_shmem_helper] [101.989535] drm_gem_vmap+0x26/0x60 [drm] [101.989594] drm_gem_fb_vmap+0x47/0x150 [drm_kms_helper] [101.989630] gud_prep_flush+0xc1/0x710 [gud] [101.989639] ? _raw_spin_lock+0x17/0x40 [101.989648] gud_flush_work+0x1e0/0x430 [gud] [101.989653] ? __switch_to+0x11d/0x470 [101.989664] process_one_work+0x21f/0x3f0 [101.989673] worker_thread+0x200/0x3e0 [101.989679] ? rescuer_thread+0x390/0x390 [101.989684] kthread+0xfd/0x130 [101.989690] ? kthread_complete_and_exit+0x20/0x20 [101.989696] ret_from_fork+0x22/0x30 [101.989706] </TASK> [101.989708] == The source of this warning is in iosys_map_clear() called from dma_buf_vmap(). It conditionally sets values based on map->is_iomem. The iosys_map variables are allocated uninitialized on the stack leading to ->is_iomem having all kinds of values and not only 0/1. Fix this by zeroing the iosys_map variables.	N/A	More Details
CVE-2022-50629	In the Linux kernel, the following vulnerability has been resolved: wifi: rsi: Fix memory leak in rsi_coex_attach() The coex_cb needs to be freed when rsi_create_kthread() failed in rsi_coex_attach().	N/A	More Details
CVE-2022-50630	In the Linux kernel, the following vulnerability has been resolved: mm: hugetlb: fix UAF in hugetlb_handle_userfault The vma_lock and hugetlb_fault_mutex are dropped before handling userfault and reacquire them again after handle_userfault(), but reacquire the vma_lock could lead to UAF[1,2] due to the following race, hugetlb_fault hugetlb_no_page /*unlock vma_lock */ hugetlb_handle_userfault handle_userfault /* unlock mm->mmap_lock*/ vm_mmap_pgoff do_mmap mmap_region munmap_vma_range /* clean old vma */ /* lock vma_lock again <--- UAF */ /* unlock vma_lock */ Since the vma_lock will unlock immediately after hugetlb_handle_userfault(), let's drop the unneeded lock and unlock in hugetlb_handle_userfault() to fix the issue. [1] https://lore.kernel.org/linux-mm/000000000000d5e00a05e834962e@google.com/ [2] https://lore.kernel.org/linux-mm/20220921014457.1668-1-liuzixian4@huawei.com/	N/A	More Details
CVE-2023-53742	In the Linux kernel, the following vulnerability has been resolved: kcsan: Avoid READ_ONCE() in read_instrumented_memory() Haibo Li reported: | Unable to handle kernel paging request at virtual address | ffffff802a0d8d7171 | Mem abort info:o: | ESR = 0x9600002121 | EC = 0x25: DABT (current EL), IL = 32 bitsts | SET = 0, FnV = 0 0 | EA = 0, S1PTW = 0 0 | FSC = 0x21: alignment fault | Data abort info:o: | ISV = 0, ISS = 0x0000002121 | CM = 0, WnR = 0 0 | swapper pgtable: 4k pages, 39-bit VAs, pgdp=0000000002835200000 | [ffffff802a0d8d71] pgd=180000005fbf9003, p4d=180000005fbf9003, | pud=180000005fbf9003, pmd=180000005fbe8003, pte=006800002a0d8707 | Internal error: Oops: 96000021 [#1] PREEMPT SMP | Modules linked in: | CPU: 2 PID: 45 Comm: kworker/u8:2 Not tainted | 5.15.78-android13-8-g63561175bbda-dirty #1 | ... | pc : kcsan_setup_watchpoint+0x26c/0x6bc | lr : kcsan_setup_watchpoint+0x88/0x6bc | sp : ffffffc00ab4b7f0 | x29: ffffffc00ab4b800 x28: ffffff80294fe588 x27: 0000000000000001 | x26: 0000000000000019 x25: 0000000000000001 x24: ffffff80294fdb80 | x23: 0000000000000000 x22: ffffffc00a70fb68 x21: ffffff802a0d8d71 | x20: 0000000000000002 x19: 0000000000000000 x18: ffffffc00a9bd060 | x17: 0000000000000001 x16: 0000000000000000 x15: ffffffc00a59f000 | x14: 0000000000000001 x13: 0000000000000000 x12: ffffffc00a70faa0 | x11: 00000000aaaaaaab x10: 0000000000000054 x9 : ffffffc00839adf8 | x8 : ffffffc009b4cf00 x7 : 0000000000000000 x6 : 0000000000000007 | x5 : 0000000000000000 x4 : 0000000000000000 x3 : ffffffc00a70fb70 | x2 : 0005ff802a0d8d71 x1 : 0000000000000000 x0 : 0000000000000000 | Call trace: | kcsan_setup_watchpoint+0x26c/0x6bc | __tsan_read2+0x1f0/0x234 | inflate_fast+0x498/0x750 | zlib_inflate+0x1304/0x2384 | __gunzip+0x3a0/0x45c | gunzip+0x20/0x30 | unpack_to_rootfs+0x2a8/0x3fc | do_populate_rootfs+0xe8/0x11c | async_run_entry_fn+0x58/0x1bc | process_one_work+0x3ec/0x738 | worker_thread+0x4c4/0x838 | kthread+0x20c/0x258 | ret_from_fork+0x10/0x20 | Code: b8bfc2a8 2a0803f7 14000007 d503249f (78bfc2a8)) | ---[end trace 613a943cb0a572b6]----- The reason for this is that on certain arm64 configuration since e35123d83ee3 ("arm64: lto: Strengthen READ_ONCE() to acquire when CONFIG_LTO=y"), READ_ONCE() may be promoted to a full atomic acquire instruction which cannot be used on unaligned addresses. Fix it by avoiding READ_ONCE() in read_instrumented_memory(), and simply forcing the compiler to do the required access by casting to the appropriate volatile type. In terms of generated code this currently only affects architectures that do not use the default READ_ONCE() implementation. The only downside is that we are not guaranteed atomicity of the access itself, although on most architectures a plain load up to machine word size should still be atomic (a fact the default READ_ONCE() still relies on itself).	N/A	More Details
CVE-2023-53743	In the Linux kernel, the following vulnerability has been resolved: PCI: Free released resource after coalescing release_resource() doesn't actually free the resource or resource list entry so free the resource list entry to avoid a leak.	N/A	More Details
CVE-2023-53744	In the Linux kernel, the following vulnerability has been resolved: soc: ti: pm33xx: Fix refcount leak in am33xx_pm_probe wkup_m3_ipc_get() takes refcount, which should be freed by wkup_m3_ipc_put(). Add missing refcount release in the error paths.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: um: vector: Fix memory leak in vector_config If the return value of the		More

2023-53745	uml_parse_vector_ifspec function is NULL, we should call kfree(params) to prevent memory leak.	N/A	Details
CVE-2023-53746	In the Linux kernel, the following vulnerability has been resolved: s390/vfio-ap: fix memory leak in vfio_ap device driver The device release callback function invoked to release the matrix device uses the dev_get_drvdata(device *dev) function to retrieve the pointer to the vfio_matrix_dev object in order to free its storage. The problem is, this object is not stored as drvdata with the device; since the kfree function will accept a NULL pointer, the memory for the vfio_matrix_dev object is never freed. Since the device being released is contained within the vfio_matrix_dev object, the container_of macro will be used to retrieve its pointer.	N/A	More Details
CVE-2023-53747	In the Linux kernel, the following vulnerability has been resolved: vc_screen: reload load of struct vc_data pointer in vcs_write() to avoid UAF After a call to console_unlock() in vcs_write() the vc_data struct can be freed by vc_port_destruct(). Because of that, the struct vc_data pointer must be reloaded in the while loop in vcs_write() after console_lock() to avoid a UAF when vcs_size() is called. Syzkaller reported a UAF in vcs_size(). BUG: KASAN: slab-use-after-free in vcs_size (drivers/tty/vt/vc_screen.c:215) Read of size 4 at addr ffff8880beab89a8 by task repro_vcs_size/4119 Call Trace: <TASK> __asan_report_load4_noabort (mm/kasan/report_generic.c:380) vcs_size (drivers/tty/vt/vc_screen.c:215) vcs_write (drivers/tty/vt/vc_screen.c:664) vfs_write (fs/read_write.c:582 fs/read_write.c:564) ... <TASK> Allocated by task 1213: kmalloc_trace (mm/slab_common.c:1064) vc_allocate (./include/linux/slab.h:559 ./include/linux/slab.h:680 drivers/tty/vt/vt.c:1078 drivers/tty/vt/vt.c:1058) con_install (drivers/tty/vt/vt.c:3334) tty_init_dev (drivers/tty/tty_io.c:1303 drivers/tty/tty_io.c:1415 drivers/tty/tty_io.c:1392) tty_open (drivers/tty/tty_io.c:2082 drivers/tty/tty_io.c:2128) chrdev_open (fs/char_dev.c:415) do_dentry_open (fs/open.c:921) vfs_open (fs/open.c:1052) ... Freed by task 4116: kfree (mm/slab_common.c:1016) vc_port_destruct (drivers/tty/vt/vt.c:1044) tty_port_destructor (drivers/tty/tty_port.c:296) tty_port_put (drivers/tty/tty_port.c:312) vt_disallocate_all (drivers/tty/vt/vt_ioctl.c:662 (discriminator 2)) vt_ioctl (drivers/tty/vt/vt_ioctl.c:903) tty_ioctl (drivers/tty/tty_io.c:2778) ... The buggy address belongs to the object at ffff8880beab8800 which belongs to the cache kmalloc-1k of size 1024 The buggy address is located 424 bytes inside of freed 1024-byte region [ffff8880beab8800, ffff8880beab8c00) The buggy address belongs to the physical page: page:00000000afc77580 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0xbeab8 head:00000000afc77580 order:3 entire_mapcount:0 nr_pages_mapped:0 pincount:0 flags: 0xfffffc0010200(slab|head|node=0|zone=1|lastcpupid=0x1fffff) page_type: 0xffffffff() raw: 000fffffc0010200 ffff888100042dc0 ffffea000426de00 dead000000000002 raw: 0000000000000000 0000000000100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8880beab8880: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8880beab8900: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8880beab8980: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8880beab8a00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8880beab8a80: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == Disabling lock debugging due to kernel taint	N/A	More Details
CVE-2023-53749	In the Linux kernel, the following vulnerability has been resolved: x86: fix clear_user_rep_good() exception handling annotation This code no longer exists in mainline, because it was removed in commit d2c95f9d6802 ("x86: don't use REP_GOOD or ERMS for user memory clearing") upstream. However, rather than backport the full range of x86 memory clearing and copying cleanups, fix the exception table annotation placement for the final 'rep movsb' in clear_user_rep_good(): rather than pointing at the actual instruction that did the user space access, it pointed to the register move just before it. That made sense from a code flow standpoint, but not from an actual usage standpoint: it means that if user access takes an exception, the exception handler won't actually find the instruction in the exception tables. As a result, rather than fixing it up and returning -EFAULT, it would then turn it into a kernel oops report instead, something like: BUG: unable to handle page fault for address: 0000000020081000 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page ... RIP: 0010:clear_user_rep_good+0x1c/0x30 arch/x86/lib/clear_page_64.S:147 ... Call Trace: __clear_user arch/x86/include/asm/uaccess_64.h:103 [inline] clear_user arch/x86/include/asm/uaccess_64.h:124 [inline] iov_iter_zero+0x709/0x1290 lib/iov_iter.c:800 iomap_dio_hole_iter fs/iomap/direct-io.c:389 [inline] iomap_dio_iter fs/iomap/direct-io.c:440 [inline] __iomap_dio_rw+0xe3d/0x1cd0 fs/iomap/direct-io.c:601 iomap_dio_rw+0x40/0xa0 fs/iomap/direct-io.c:689 ext4_dio_read_iter fs/ext4/file.c:94 [inline] ext4_file_read_iter+0x4be/0x690 fs/ext4/file.c:145 call_read_iter include/linux/fs.h:2183 [inline] do_iter_readv_writev+0x2e0/0x3b0 fs/read_write.c:733 do_iter_read+0x2f2/0x750 fs/read_write.c:796 vfs_readv+0xe5/0x150 fs/read_write.c:916 do_preadv+0x1b6/0x270 fs/read_write.c:1008 __do_sys_preadv2 fs/read_write.c:1070 [inline] __se_sys_preadv2 fs/read_write.c:1061 [inline] __x64_sys_preadv2+0xef/0x150 fs/read_write.c:1061 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x39/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd which then looks like a filesystem bug rather than the incorrect exception annotation that it is. [The alternative to this one-liner fix is to take the upstream series that cleans this all up: 68674f94ffc9 ("x86: don't use REP_GOOD or ERMS for small memory copies") 20f3337d350c ("x86: don't use REP_GOOD or ERMS for small memory clearing") adfcf4231b8c ("x86: don't use REP_GOOD or ERMS for user memory copies") * d2c95f9d6802 ("x86: don't use REP_GOOD or ERMS for user memory clearing") 3639a535587d ("x86: move stac/clac from user copy routines into callers") 577e6a7fd50d ("x86: inline the 'rep movs' in user copies for the FSRM case") 8c9b6a88b7e2 ("x86: improve on the non-rep 'clear_user' function") 427fda2c8a49 ("x86: improve on the non-rep 'copy_user' function") * e046fe5a36a9 ("x86: set FSRS automatically on AMD CPUs that have FSRM") e1f2750edc4a ("x86: remove 'zerorest' argument from __copy_user_nocache()") 034ff37d3407 ("x86: rewrite '__copy_user_nocache' function") with either the whole series or at a minimum the two marked commits being needed to fix this issue]	N/A	More Details
CVE-2023-53759	In the Linux kernel, the following vulnerability has been resolved: HID: hidraw: fix data race on device refcount The hidraw_open() function increments the hidraw device reference counter. The counter has no dedicated synchronization mechanism, resulting in a potential data race when concurrently opening a device. The race is a regression introduced by commit 8590222e4b02 ("HID: hidraw: Replace hidraw device table mutex with a rwsem"). While minors_rwsem is intended to protect the hidraw_table itself, by instead acquiring the lock for writing, the reference counter is also protected. This is symmetrical to hidraw_release().	N/A	More Details
CVE-2023-53750	In the Linux kernel, the following vulnerability has been resolved: pinctrl: freescale: Fix a memory out of bounds when num_configs is 1 The config passed in by pad wakeup is 1, when num_configs is 1, Configuration [1] should not be fetched, which will be detected by KASAN as a memory out of bounds condition. Modify to get configs[1] when num_configs is 2.	N/A	More Details
CVE-2023-53751	In the Linux kernel, the following vulnerability has been resolved: cifs: fix potential use-after-free bugs in TCP_Server_Info::hostname TCP_Server_Info::hostname may be updated once or many times during reconnect, so protect its access outside reconnect path as well and then prevent any potential use-after-free bugs.	N/A	More Details
CVE-2023-	In the Linux kernel, the following vulnerability has been resolved: net: deal with integer overflows in kmalloc_reserve() Blamed commit changed: ptr = kmalloc(size); if (ptr) size = ksize(ptr); size = kmalloc_size_roundup(size); ptr = kmalloc(size); This allowed various crash as reported by syzbot [1] and Kyle Zeng. Problem is that if @size is bigger than 0x80000001, kmalloc_size_roundup(size) returns 2^32. kmalloc_reserve() uses a 32bit variable (obj_size), so 2^32 is truncated to 0. kmalloc(0) returns ZERO_SIZE_PTR which is not handled by skb allocations. Following trace can be triggered if a netdev->mtu is set close to 0x7fffffff We might in the future limit netdev->mtu to more sensible limit (like KMALLOC_MAX_SIZE). This patch is based on a syzbot report, and also a report and tentative fix from Kyle Zeng. [1] BUG: KASAN: user-memory-access in __build_skb_around net/core/skbuff.c:294 [inline] BUG: KASAN: user-memory-access in __alloc_skb+0x3c4/0x6e8 net/core/skbuff.c:527 Write of size 32 at addr 00000000fffffd10 by task syz-executor.4/22554 CPU: 1 PID: 22554 Comm: syz-executor.4 Not tainted 6.1.39-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/03/2023 Call trace: dump_backtrace+0x1c8/0x1f4 arch/arm64/kernel/stacktrace.c:279 show_stack+0x2c/0x3c arch/arm64/kernel/stacktrace.c:286 __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x120/0x1a0 lib/dump_stack.c:106 print_report+0xe4/0x4b4 mm/kasan/report.c:398 kasan_report+0x150/0x1ac mm/kasan/report.c:495 kasan_check_range+0x264/0x2a4	N/A	More Details

53752	mm/kasan/generic.c:189 memset+0x40/0x70 mm/kasan/shadow.c:44 __build_skb_around net/core/skbuff.c:294 [inline] __alloc_skb+0x3c4/0x6e8 net/core/skbuff.c:527 alloc_skb include/linux/skbuff.h:1316 [inline] igmpv3_newpack+0x104/0x1088 net/ipv4/igmp.c:359 add_grec+0x81c/0x1124 net/ipv4/igmp.c:534 igmpv3_send_cr net/ipv4/igmp.c:667 [inline] igmp_ifc_timer_expire+0x1b0/0x1008 net/ipv4/igmp.c:810 call_timer_fn+0x1c0/0x9f0 kernel/time/timer.c:1474 expire_timers kernel/time/timer.c:1519 [inline] __run_timers+0x54c/0x710 kernel/time/timer.c:1790 run_timer_softirq+0x28/0x4c kernel/time/timer.c:1803 _stext+0x380/0xfbc ____do_softirq+0x14/0x20 arch/arm64/kernel/irq.c:79 call_on_irq_stack+0x24/0x4c arch/arm64/kernel/entry.S:891 do_softirq_own_stack+0x20/0x2c arch/arm64/kernel/irq.c:84 invoke_softirq kernel/softirq.c:437 [inline] __irq_exit_rcu+0x1c0/0x4cc kernel/softirq.c:683 irq_exit_rcu+0x14/0x78 kernel/softirq.c:695 el0_interrupt+0x7c/0x2e0 arch/arm64/kernel/entry-common.c:717 __el0_irq_handler_common+0x18/0x24 arch/arm64/kernel/entry-common.c:724 el0t_64_irq_handler+0x10/0x1c arch/arm64/kernel/entry-common.c:729 el0t_64_irq+0x1a0/0x1a4 arch/arm64/kernel/entry.S:584		
CVE-2023-53753	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix mapping to non-allocated address [Why] There is an issue mapping non-allocated location of memory. It would allocate gpio registers from an array out of bounds. [How] Patch correct numbers of bounds for using.	N/A	More Details
CVE-2023-53754	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix ioremap issues in lpfc_sli4_pci_mem_setup() When if_type equals zero and pci_resource_start(pdev, PCI_64BIT_BAR4) returns false, drbl_regs_memmap_p is not remapped. This passes a NULL pointer to iounmap(), which can trigger a WARN() on certain arches. When if_type equals six and pci_resource_start(pdev, PCI_64BIT_BAR4) returns true, drbl_regs_memmap_p may has been remapped and ctrl_regs_memmap_p is not remapped. This is a resource leak and passes a NULL pointer to iounmap(). To fix these issues, we need to add null checks before iounmap(), and change some goto labels.	N/A	More Details
CVE-2023-53755	In the Linux kernel, the following vulnerability has been resolved: dmaengine: ptdma: check for null desc before calling pt_cmd_callback Resolves a panic that can occur on AMD systems, typically during host shutdown, after the PTDMA driver had been exercised. The issue was the pt_issue_pending() function is mistakenly assuming that there will be at least one descriptor in the Submitted queue when the function is called. However, it is possible that both the Submitted and Issued queues could be empty, which could result in pt_cmd_callback() being mistakenly called with a NULL pointer. Ref: Bugzilla Bug 216856.	N/A	More Details
CVE-2023-53756	In the Linux kernel, the following vulnerability has been resolved: KVM: VMX: Fix crash due to uninitialized current_vmcs KVM enables 'Enlightened VMCS' and 'Enlightened MSR Bitmap' when running as a nested hypervisor on top of Hyper-V. When MSR bitmap is updated, evmcs_touch_msr_bitmap function uses current_vmcs per-cpu variable to mark that the msr bitmap was changed. vmx_vcpu_create() modifies the msr bitmap via vmx_disable_intercept_for_msr -> vmx_msr_bitmap_l01_changed which in the end calls this function. The function checks for current_vmcs if it is null but the check is insufficient because current_vmcs is not initialized. Because of this, the code might incorrectly write to the structure pointed by current_vmcs value left by another task. Preemption is not disabled, the current task can be preempted and moved to another CPU while current_vmcs is accessed multiple times from evmcs_touch_msr_bitmap() which leads to crash. The manipulation of MSR bitmaps by callers happens only for vmcs01 so the solution is to use vmx->vmcs01.vmcs instead of current_vmcs. BUG: kernel NULL pointer dereference, address: 0000000000000338 PGD 4e1775067 P4D 0 Oops: 0002 [#1] PREEMPT SMP NOPTI ... RIP: 0010:vmx_msr_bitmap_l01_changed+0x39/0x50 [kvm_intel] ... Call Trace: vmx_disable_intercept_for_msr+0x36/0x260 [kvm_intel] vmx_vcpu_create+0xe6/0x540 [kvm_intel] kvm_arch_vcpu_create+0x1d1/0x2e0 [kvm] kvm_vm_ioctl_create_vcpu+0x178/0x430 [kvm] kvm_vm_ioctl+0x53f/0x790 [kvm] __x64_sys_ioctl+0x8a/0xc0 do_syscall_64+0x5c/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd	N/A	More Details
CVE-2023-53757	In the Linux kernel, the following vulnerability has been resolved: irqchip/irq-mvebu-gicp: Fix refcount leak in mvebu_gicp_probe of_irq_find_parent() returns a node pointer with refcount incremented, We should use of_node_put() on it when not needed anymore. Add missing of_node_put() to avoid refcount leak.	N/A	More Details
CVE-2023-53758	In the Linux kernel, the following vulnerability has been resolved: spi: atmel-quadspi: Free resources even if runtime resume failed in .remove() An early error exit in atmel_qspi_remove() doesn't prevent the device unbind. So this results in an spi controller with an unbound parent and unmapped register space (because devm_ioremap_resource() is undone). So using the remaining spi controller probably results in an oops. Instead unregister the controller unconditionally and only skip hardware access and clk disable. Also add a warning about resume failing and return zero unconditionally. The latter has the only effect to suppress a less helpful error message by the spi core.	N/A	More Details
CVE-2025-66538	Rejected reason: Not used	N/A	More Details
CVE-2025-66537	Rejected reason: Not used	N/A	More Details
CVE-2025-66536	Rejected reason: Not used	N/A	More Details
CVE-2022-50646	In the Linux kernel, the following vulnerability has been resolved: scsi: hpsa: Fix possible memory leak in hpsa_init_one() The hpda_alloc_ctlr_info() allocates h and its field reply_map. However, in hpsa_init_one(), if alloc_percpu() failed, the hpsa_init_one() jumps to clean1 directly, which frees h and leaks the h->reply_map. Fix by calling hpda_free_ctlr_info() to release h->replay_map and h instead free h directly.	N/A	More Details
CVE-2022-50637	In the Linux kernel, the following vulnerability has been resolved: cpufreq: qcom-hw: Fix memory leak in qcom_cpufreq_hw_read_lut() If "cpu_dev" fails to get opp table in qcom_cpufreq_hw_read_lut(), the program will return, resulting in "table" resource is not released.	N/A	More Details
CVE-2022-	In the Linux kernel, the following vulnerability has been resolved: ext4: fix bug_on in __es_tree_search caused by bad boot loader inode We got a issue as fllows: == kernel BUG at fs/ext4/extents_status.c:203! invalid opcode: 0000 [#1] PREEMPT SMP CPU: 1 PID: 945 Comm: cat Not tainted 6.0.0-next-20221007-dirty #349 RIP: 0010:ext4_es_end.isra.0+0x34/0x42 RSP: 0018:ffffc9000143b768 EFLAGS: 00010203 RAX: 0000000000000000 RBX: ffff8881769cd0b8 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffffffff8fc27cf7 RDI: 00000000ffffffff RBP: ffff8881769cd0bc R08: 0000000000000000 R09: ffffc9000143b5f8 R10: 0000000000000001 R11: 0000000000000001 R12: ffff8881769cd0a0 R13: ffff8881768e5668 R14: 00000000768e52f0 R15: 0000000000000000 FS: 00007f359f7f05c0(0000)GS:ffff88842fd00000(0000)knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f359f5a2000 CR3: 000000017130c000 CR4: 00000000000006e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __es_tree_search.isra.0+0x6d/0xf5 ext4_es_cache_extent+0xfa/0x230 ext4_cache_extents+0xd2/0x110 ext4_find_extent+0x5d5/0x8c0 ext4_ext_map_blocks+0x9c/0x1d30 ext4_map_blocks+0x431/0xa50 ext4_mpage_readpages+0x48e/0xe40 ext4_readahead+0x47/0x50 read_pages+0x82/0x530 page_cache_ra_unbounded+0x199/0x2a0 do_page_cache_ra+0x47/0x70 page_cache_ra_order+0x242/0x400	N/A	More

50638	ondemand_readahead+0x1e8/0x4b0 page_cache_sync_ra+0xf4/0x110 filemap_get_pages+0x131/0xb20 filemap_read+0xda/0x4b0 generic_file_read_iter+0x13a/0x250 ext4_file_read_iter+0x59/0x1d0 vfs_read+0x28f/0x460 ksys_read+0x73/0x160 __x64_sys_read+0x1e/0x30 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd </TASK> == In the above issue, ioctl invokes the swap_inode_boot_loader function to swap inode<5> and inode<12>. However, inode<5> contain incorrect imode and disordered extents, and i_nlink is set to 1. The extents check for inode in the ext4_iget function can be bypassed bacause 5 is EXT4_BOOT_LOADER_INO. While links_count is set to 1, the extents are not initialized in swap_inode_boot_loader. After the ioctl command is executed successfully, the extents are swapped to inode<12>, in this case, run the `cat` command to view inode<12>. And Bug_ON is triggered due to the incorrect extents. When the boot loader inode is not initialized, its imode can be one of the following: 1) the imode is a bad type, which is marked as bad_inode in ext4_iget and set to S_IFREG. 2) the imode is good type but not S_IFREG. 3) the imode is S_IFREG. The BUG_ON may be triggered by bypassing the check in cases 1 and 2. Therefore, when the boot loader inode is bad_inode or its imode is not S_IFREG, initialize the inode to avoid triggering the BUG.		Details
CVE-2022-50639	In the Linux kernel, the following vulnerability has been resolved: io-wq: Fix memory leak in worker creation If the CPU mask allocation for a node fails, then the memory allocated for the 'io_wqe' struct of the current node doesn't get freed on the error handling path, since it has not yet been added to the 'wqes' array. This was spotted when fuzzing v6.1-rc1 with Syzkaller: BUG: memory leak unreferenced object 0xffff8880093d5000 (size 1024): comm "syz-executor.2", pid 7701, jiffies 4295048595 (age 13.900s) 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: [<00000000cb463369>] __kmem_cache_alloc_node+0x18e/0x720 [<00000000147a3f9c>] kmalloc_node_trace+0x2a/0x130 [<000000004e107011>] io_wq_create+0x7b9/0xdc0 [<00000000c38b2018>] io_uring_alloc_task_context+0x31e/0x59d [<00000000867399da>] __io_uring_add_tctx_node.cold+0x19/0x1ba [<000000007e0e7a79>] io_uring_setup.cold+0x1b80/0x1dce [<00000000b545e9f6>] __x64_sys_io_uring_setup+0x5d/0x80 [<000000008a8a7508>] do_syscall_64+0x5d/0x90 [<000000004ac08bec>] entry_SYSCALL_64_after_hwframe+0x63/0xcd	N/A	More Details
CVE-2022-50640	In the Linux kernel, the following vulnerability has been resolved: mmc: core: Fix kernel panic when remove non-standard SDIO card SDIO tuple is only allocated for standard SDIO card, especially it causes memory corruption issues when the non-standard SDIO card has removed, which is because the card device's reference counter does not increase for it at sdio_init_func(), but all SDIO card device reference counter gets decreased at sdio_release_func().	N/A	More Details
CVE-2022-50641	In the Linux kernel, the following vulnerability has been resolved: HSI: omap_ssi: Fix refcount leak in ssi_probe When returning or breaking early from a for_each_available_child_of_node() loop, we need to explicitly call of_node_put() on the child node to possibly release the node.	N/A	More Details
CVE-2022-50642	In the Linux kernel, the following vulnerability has been resolved: platform/chrome: cros_ec_typec: zero out stale pointers `cros_typec_get_switch_handles` allocates four pointers when obtaining type-c switch handles. These pointers are all freed if failing to obtain any of them; therefore, pointers in `port` become stale. The stale pointers eventually cause use-after-free or double free in later code paths. Zeroing out all pointer fields after freeing to eliminate these stale pointers.	N/A	More Details
CVE-2022-50643	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix xid leak in cifs_copy_file_range() If the file is used by swap, before return -EOPNOTSUPP, should free the xid, otherwise, the xid will be leaked.	N/A	More Details
CVE-2022-50644	In the Linux kernel, the following vulnerability has been resolved: clk: ti: dra7-atl: Fix reference leak in of_dra7_atl_clk_probe pm_runtime_get_sync() will increment pm usage counter. Forgetting to putting operation will result in reference leak. Add missing pm_runtime_put_sync in some error paths.	N/A	More Details
CVE-2022-50645	In the Linux kernel, the following vulnerability has been resolved: EDAC/i10nm: fix refcount leak in pci_get_dev_wrapper() As the comment of pci_get_domain_bus_and_slot() says, it returns a PCI device with refcount incremented, so it doesn't need to call an extra pci_dev_get() in pci_get_dev_wrapper(), and the PCI device needs to be put in the error path.	N/A	More Details
CVE-2022-50647	In the Linux kernel, the following vulnerability has been resolved: RISC-V: Make port I/O string accessors actually work Fix port I/O string accessors such as `insb', `outsb', etc. which use the physical PCI port I/O address rather than the corresponding memory mapping to get at the requested location, which in turn breaks at least accesses made by our parport driver to a PCIe parallel port such as: PCI parallel port detected: 1415:c118, I/O at 0x1000(0x1008), IRQ 20 parport0: PC-style at 0x1000 (0x1008), irq 20, using FIFO [PCSPP,TRISTATE,COMPAT,EPP,ECP] causing a memory access fault: Unable to handle kernel access to user memory without uaccess routines at virtual address 0000000000001008 Oops [#1] Modules linked in: CPU: 1 PID: 350 Comm: cat Not tainted 6.0.0-rc2-00283-g10d4879f9ef0-dirty #23 Hardware name: SiFive HiFive Unmatched A00 (DT) epc : parport_pc_fifo_write_block_pio+0x266/0x416 ra : parport_pc_fifo_write_block_pio+0xb4/0x416 epc : ffffffff80542c3e ra : ffffffff80542a8c sp : ffffffd88899fc60 gp : ffffffff80fa2700 tp : ffffffd882b1e900 t0 : ffffffd883d0b000 t1 : fffffffff000002 t2 : 4646393043330a38 s0 : ffffffd88899fcf0 s1 : 0000000000001000 a0 : 0000000000000010 a1 : 0000000000000000 a2 : ffffffd883d0a010 a3 : 0000000000000023 a4 : 00000000ffff8fbb a5 : ffffffd883d0a001 a6 : 0000000100000000 a7 : ffffffc800000000 s2 : fffffffff000002 s3 : ffffffff80d28880 s4 : ffffffff80fa1f50 s5 : 0000000000001008 s6 : 0000000000000008 s7 : ffffffd883d0a000 s8 : 0004000000000000 s9 : ffffffff80dc1d80 s10: ffffffd8807e4000 s11: 0000000000000000 t3 : 00000000000000ff t4 : 393044410a303930 t5 : 0000000000001000 t6 : 0000000000040000 status: 0000000200000120 badaddr: 0000000000001008 cause: 000000000000000f [<ffffffff80543212>] parport_pc_compat_write_block_pio+0xfe/0x200 [<ffffffff8053bbc0>] parport_write+0x46/0xf8 [<ffffffff8050530e>] lp_write+0x158/0x2d2 [<ffffffff80185716>] vfs_write+0x8e/0x2c2 [<ffffffff80185a74>] ksys_write+0x52/0xc2 [<ffffffff80185af2>] sys_write+0xe/0x16 [<ffffffff80003770>] ret_from_syscall+0x0/0x2 ---[end trace 0000000000000000]--- For simplicity address the problem by adding PCI_IOBASE to the physical address requested in the respective wrapper macros only, observing that the raw accessors such as `__insb', `__outsb', etc. are not supposed to be used other than by said macros. Remove the cast to `long' that is no longer needed on `addr' now that it is used as an offset from PCI_IOBASE and add parentheses around `addr' needed for predictable evaluation in macro expansion. No need to make said adjustments in separate changes given that current code is gravely broken and does not ever work.	N/A	More Details
CVE-2022-50635	In the Linux kernel, the following vulnerability has been resolved: powerpc/kprobes: Fix null pointer reference in arch_prepare_kprobe() I found a null pointer reference in arch_prepare_kprobe(): # echo 'p cmdline_proc_show' > kprobe_events # echo 'p cmdline_proc_show+16' >> kprobe_events Kernel attempted to read user page (0) - exploit attempt? (uid: 0) BUG: Kernel NULL pointer dereference on read at 0x00000000 Faulting instruction address: 0xc000000000050bfc Oops: Kernel access of bad area, sig: 11 [#1] LE PAGE_SIZE=64K MMU=Radix SMP NR_CPUS=2048 NUMA PowerNV Modules linked in: CPU: 0 PID: 122 Comm: sh Not tainted 6.0.0-rc3-00007-gdcf8e5633e2e #10 NIP: c000000000050bfc LR: c000000000050bec CTR: 0000000000005bdc REGS: c0000000348475b0 TRAP: 0300 Not tainted (6.0.0-rc3-00007-gdcf8e5633e2e) MSR: 9000000000009033 <SF,HV,EE,ME,IR,DR,RI,LE> CR: 88002444 XER: 20040006 CFAR: c00000000022d100 DAR: 0000000000000000 DSISR: 40000000 IRQMASK: 0 ... NIP arch_prepare_kprobe+0x10c/0x2d0 LR arch_prepare_kprobe+0xfc/0x2d0 Call Trace: 0xc0000000012f77a0 (unreliable) register_kprobe+0x3c0/0x7a0 __register_trace_kprobe+0x140/0x1a0 __trace_kprobe_create+0x794/0x1040 trace_probe_create+0xc4/0xe0 create_or_delete_trace_kprobe+0x2c/0x80 trace_parse_run_command+0xf0/0x210 probes_write+0x20/0x40 vfs_write+0xfc/0x450 ksys_write+0x84/0x140 system_call_exception+0x17c/0x3a0 system_call_vectored_common+0xe8/0x278 --- interrupt: 3000 at 0x7fffa5682de0 NIP: 00007fffa5682de0 LR: 0000000000000000 CTR: 0000000000000000 REGS: c000000034847e80 TRAP: 3000 Not	N/A	More Details

	tainted (6.0.0-rc3-00007-gdcf8e5633e2e) MSR: 900000000280f033 <SF,HV,VEC,VSX,EE,PR,FP,ME,IR,DR,RI,LE> CR: 44002408 XER: 00000000 The address being probed has some special: cmdline_proc_show: Probe based on ftrace cmdline_proc_show+16: Probe for the next instruction at the ftrace location The ftrace-based kprobe does not generate kprobe::ainsn::insn, it gets set to NULL. In arch_prepare_kprobe() it will check for: ... prev = get_kprobe(p->addr - 1); preempt_enable_no_resched(); if (prev && ppc_inst_prefixed(ppc_inst_read(prev->ainsn.insn))) { ... If prev is based on ftrace, 'ppc_inst_read(prev->ainsn.insn)' will occur with a null pointer reference. At this point prev->addr will not be a prefixed instruction, so the check can be skipped. Check if prev is ftrace-based kprobe before reading 'prev->ainsn.insn' to fix this problem. [mpe: Trim oops]		
CVE-2022-50648	In the Linux kernel, the following vulnerability has been resolved: ftrace: Fix recursive locking direct_mutex in ftrace_modify_direct_caller Naveen reported recursive locking of direct_mutex with sample ftrace-direct-modify.ko: [74.762406] WARNING: possible recursive locking detected [74.762887] 6.0.0-rc6+ #33 Not tainted [74.763216] ---------- [74.763672] event-sample-fn/1084 is trying to acquire lock: [74.764152] ffffffff86c9d6b0 (direct_mutex){+.+.}-{3:3}, at: \ register_ftrace_function+0x1f/0x180 [74.764922] [74.764922] but task is already holding lock: [74.765421] ffffffff86c9d6b0 (direct_mutex){+.+.}-{3:3}, at: \ modify_ftrace_direct+0x34/0x1f0 [74.766142] [74.766142] other info that might help us debug this: [74.766701] Possible unsafe locking scenario: [74.766701] [74.767216] CPU0 [74.767437] ---- [74.767656] lock(direct_mutex); [74.767952] lock(direct_mutex); [74.768245] [74.768245] *** DEADLOCK *** [74.768245] [74.768750] May be due to missing lock nesting notation [74.768750] [74.769332] 1 lock held by event-sample-fn/1084: [74.769731] #0: ffffffff86c9d6b0 (direct_mutex){+.+.}-{3:3}, at: \ modify_ftrace_direct+0x34/0x1f0 [74.770496] [74.770496] stack backtrace: [74.770884] CPU: 4 PID: 1084 Comm: event-sample-fn Not tainted ... [74.771498] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), ... [74.772474] Call Trace: [74.772696] <TASK> [74.772896] dump_stack_lvl+0x44/0x5b [74.773223] __lock_acquire.cold.74+0xac/0x2b7 [74.773616] lock_acquire+0xd2/0x310 [74.773936] ? register_ftrace_function+0x1f/0x180 [74.774357] ? lock_is_held_type+0xd8/0x130 [74.774744] ? my_tramp2+0x11/0x11 [ftrace_direct_modify] [74.775213] __mutex_lock+0x99/0x1010 [74.775536] ? register_ftrace_function+0x1f/0x180 [74.775954] ? slab_free_freelist_hook.isra.43+0x115/0x160 [74.776424] ? ftrace_set_hash+0x195/0x220 [74.776779] ? register_ftrace_function+0x1f/0x180 [74.777194] ? kfree+0x3e1/0x440 [74.777482] ? my_tramp2+0x11/0x11 [ftrace_direct_modify] [74.777941] ? __schedule+0xb40/0xb40 [74.778258] ? register_ftrace_function+0x1f/0x180 [74.778672] ? my_tramp1+0xf/0xf [ftrace_direct_modify] [74.779128] register_ftrace_function+0x1f/0x180 [74.779527] ? ftrace_set_filter_ip+0x33/0x70 [74.779910] ? __schedule+0xb40/0xb40 [74.780231] ? my_tramp1+0xf/0xf [ftrace_direct_modify] [74.780678] ? my_tramp2+0x11/0x11 [ftrace_direct_modify] [74.781147] ftrace_modify_direct_caller+0x5b/0x90 [74.781563] ? 0xffffffffa0201000 [74.781859] ? my_tramp1+0xf/0xf [ftrace_direct_modify] [74.782309] modify_ftrace_direct+0x1b2/0x1f0 [74.782690] ? __schedule+0xb40/0xb40 [74.783014] ? simple_thread+0x2a/0xb0 [ftrace_direct_modify] [74.783508] ? __schedule+0xb40/0xb40 [74.783832] ? my_tramp2+0x11/0x11 [ftrace_direct_modify] [74.784294] simple_thread+0x76/0xb0 [ftrace_direct_modify] [74.784766] kthread+0xf5/0x120 [74.785052] ? kthread_complete_and_exit+0x20/0x20 [74.785464] ret_from_fork+0x22/0x30 [74.785781] </TASK> Fix this by using register_ftrace_function_nolock in ftrace_modify_direct_caller.	N/A	More Details
CVE-2022-50649	In the Linux kernel, the following vulnerability has been resolved: power: supply: adp5061: fix out-of-bounds read in adp5061_get_chg_type() ADP5061_CHG_STATUS_1_CHG_STATUS is masked with 0x07, which means a length of 8, but adp5061_chg_type array size is 4, may end up reading 4 elements beyond the end of the adp5061_chg_type[] array.	N/A	More Details
CVE-2022-50650	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix reference state management for synchronous callbacks Currently, verifier verifies callback functions (sync and async) as if they will be executed once, (i.e. it explores execution state as if the function was being called once). The next insn to explore is set to start of subprog and the exit from nested frame is handled using curframe > 0 and prepare_func_exit. In case of async callback it uses a customized variant of push_stack simulating a kind of branch to set up custom state and execution context for the async callback. While this approach is simple and works when callback really will be executed only once, it is unsafe for all of our current helpers which are for_each style, i.e. they execute the callback multiple times. A callback releasing acquired references of the caller may do so multiple times, but currently verifier sees it as one call inside the frame, which then returns to caller. Hence, it thinks it released some reference that the cb e.g. got access through callback_ctx (register filled inside cb from spilled typed register on stack). Similarly, it may see that an acquire call is unpaired inside the callback, so the caller will copy the reference state of callback and then will have to release the register with new ref_obj_ids. But again, the callback may execute multiple times, but the verifier will only account for acquired references for a single symbolic execution of the callback, which will cause leaks. Note that for async callback case, things are different. While currently we have bpf_timer_set_callback which only executes it once, even for multiple executions it would be safe, as reference state is NULL and check_reference_leak would force program to release state before BPF_EXIT. The state is also unaffected by analysis for the caller frame. Hence async callback is safe. Since we want the reference state to be accessible, e.g. for pointers loaded from stack through callback_ctx's PTR_TO_STACK, we still have to copy caller's reference_state to callback's bpf_func_state, but we enforce that whatever references it adds to that reference_state has been released before it hits BPF_EXIT. This requires introducing a new callback_ref member in the reference state to distinguish between caller vs callee references. Hence, check_reference_leak now errors out if it sees we are in callback_fn and we have not released callback_ref refs. Since there can be multiple nested callbacks, like frame 0 -> cb1 -> cb2 etc. we need to also distinguish between whether this particular ref belongs to this callback frame or parent, and only error for our own, so we store state->frameno (which is always non-zero for callbacks). In short, callbacks can read parent reference_state, but cannot mutate it, to be able to use pointers acquired by the caller. They must only undo their changes (by releasing their own acquired_refs before BPF_EXIT) on top of caller reference_state before returning (at which point the caller and callback state will match anyway, so no need to copy it back to caller).	N/A	More Details
CVE-2022-50651	In the Linux kernel, the following vulnerability has been resolved: ethtool: eeprom: fix null-deref on genl_info in dump The similar fix as commit 46cdedf2a0fa ("ethtool: pse-pd: fix null-deref on genl_info in dump") is also needed for ethtool eeprom.	N/A	More Details
CVE-2022-50652	In the Linux kernel, the following vulnerability has been resolved: uio: uio_dmem_genirq: Fix missing unlock in irq configuration Commit b74351287d4b ("uio: fix a sleep-in-atomic-context bug in uio_dmem_genirq_irqcontrol()") started calling disable_irq() without holding the spinlock because it can sleep. However, that fix introduced another bug: if interrupt is already disabled and a new disable request comes in, then the spinlock is not unlocked: root@localhost:~# printf '\x00\x00\x00\x00' > /dev/uio0 root@localhost:~# printf '\x00\x00\x00\x00' > /dev/uio0 root@localhost:~# [14.851538] BUG: scheduling while atomic: bash/223/0x00000002 [14.851991] Modules linked in: uio_dmem_genirq uio myfpga(OE) bochs drm_vram_helper drm_ttm_helper ttm drm_kms_helper drm snd_pcm ppdev joydev psmouse snd_timer snd e1000fb_sys_fops syscopyarea parport sysfillrect soundcore sysimgblt input_leds pcspkr i2c_piix4 serio_raw floppy evbug qemu_fw_cfg mac_hid pata_acpi ip_tables x_tables autofs4 [last unloaded: parport_pc] [14.854206] CPU: 0 PID: 223 Comm: bash Tainted: G OE 6.0.0-rc7 #21 [14.854786] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [14.855664] Call Trace: [14.855861] <TASK> [14.856025] dump_stack_lvl+0x4d/0x67 [14.856325] dump_stack+0x14/0x1a [14.856583] __schedule_bug.cold+0x4b/0x5c [14.856915] __schedule+0xe81/0x13d0 [14.857199] ? idr_find+0x13/0x20 [14.857456] ? get_work_pool+0x2d/0x50 [14.857756] ? __flush_work+0x233/0x280 [14.858068] ? __schedule+0xa95/0x13d0 [14.858307] ? idr_find+0x13/0x20 [14.858519] ? get_work_pool+0x2d/0x50 [14.858798] schedule+0x6c/0x100 [14.859009] schedule_hrtimeout_range_clock+0xff/0x110 [14.859335] ? tty_write_room+0x1f/0x30 [14.859598] ? n_tty_poll+0x1ec/0x220 [14.859830] ? tty_ldisc_deref+0x1a/0x20 [14.860090] schedule_hrtimeout_range+0x17/0x20 [14.860373] do_select+0x596/0x840 [14.860627] ? __kernel_text_address+0x16/0x50 [14.860954] ? poll_freewait+0xb0/0xb0 [14.861235] ? poll_freewait+0xb0/0xb0 [14.861517] ? rpm_resume+0x49d/0x780 [14.861798] ? common_interrupt+0x59/0xa0 [14.862127] ? asm_common_interrupt+0x2b/0x40 [14.862511] ? __uart_start.isra.0+0x61/0x70 [14.862902] ? __check_object_size+0x61/0x280 [14.863255] core_sys_select+0x1c6/0x400 [14.863575] ? vfs_write+0x1c9/0x3d0 [14.863853] ? vfs_write+0x1c9/0x3d0 [14.864121] ?	N/A	More Details

	_copy_from_user+0x45/0x70 [14.864526] do_pselect.constprop.0+0xb3/0xf0 [14.864893] ? do_syscall_64+0x6d/0x90 [14.865228] ? do_syscall_64+0x6d/0x90 [14.865556] __x64_sys_pselect6+0x76/0xa0 [14.865906] do_syscall_64+0x60/0x90 [14.866214] ? syscall_exit_to_user_mode+0x2a/0x50 [14.866640] ? do_syscall_64+0x6d/0x90 [14.866972] ? do_syscall_64+0x6d/0x90 [14.867286] ? do_syscall_64+0x6d/0x90 [14.867626] entry_SYSCALL_64_after_hwframe+0x63/0xcd [...] stripped [14.872959] </TASK> ('myfpga' is a simple 'uio_dmem_genirq' driver I wrote to test this) The implementation of "uio_dmem_genirq" was based on "uio_pdrv_genirq" and it is used in a similar manner to the "uio_pdrv_genirq" driver with respect to interrupt configuration and handling. At the time "uio_dmem_genirq" was introduced, both had the same implementation of the 'uio_info' handlers irqcontrol() and handler(). Then commit 34cb27528398 ("UIO: Fix concurrency issue"), which was only applied to "uio_pdrv_genirq", ended up making them a little different. That commit, among other things, changed disable_irq() to disable_irq_nosync() in the implementation of irqcontrol(). The motivation there was to avoid a deadlock between irqcontrol() and handler(), since it added a spinlock in the irq handler, and disable_irq() waits for the completion of the irq handler. By changing disable_irq() to disable_irq_nosync() in irqcontrol(), we also avoid the sleeping-whil ---truncated---		
CVE-2022-50653	In the Linux kernel, the following vulnerability has been resolved: mmc: atmel-mci: fix return value check of mmc_add_host() mmc_add_host() may return error, if we ignore its return value, it will lead two issues: 1. The memory that allocated in mmc_alloc_host() is leaked. 2. In the remove() path, mmc_remove_host() will be called to delete device, but it's not added yet, it will lead a kernel crash because of null-ptr-deref in device_del(). So fix this by checking the return value and calling mmc_free_host() in the error path.	N/A	More Details
CVE-2022-50654	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix panic due to wrong pageattr of im->image In the scenario where livepatch and kretfunc coexist, the pageattr of im->image is rox after arch_prepare_bpf_trampoline in bpf_trampoline_update, and then modify_fentry or register_fentry returns -EAGAIN from bpf_tramp_ftrace_ops_func, the BPF_TRAMP_F_ORIG_STACK flag will be configured, and arch_prepare_bpf_trampoline will be re-executed. At this time, because the pageattr of im->image is rox, arch_prepare_bpf_trampoline will read and write im->image, which causes a fault. as follows: insmod livepatch-sample.ko # samples/livepatch/livepatch-sample.c bpftrace -e 'kretfunc:cmdline_proc_show {}' BUG: unable to handle page fault for address: ffffffffa0206000 PGD 322d067 P4D 322d067 PUD 322e063 PMD 1297e067 PTE d428061 Oops: 0003 [#1] PREEMPT SMP PTI CPU: 2 PID: 270 Comm: bpftrace Tainted: G E K 6.1.0 #5 RIP: 0010:arch_prepare_bpf_trampoline+0xed/0x8c0 RSP: 0018:ffffc90001083ad8 EFLAGS: 00010202 RAX: ffffffffa0206000 RBX: 0000000000000020 RCX: 0000000000000000 RDX: ffffffffa0206001 RSI: ffffffffa0206000 RDI: 0000000000000030 RBP: ffffc90001083b70 R08: 0000000000000066 R09: ffff88800f51b400 R10: 000000002e72c6e5 R11: 00000000d0a15080 R12: ffff8880110a68c8 R13: 0000000000000000 R14: ffff88800f51b400 R15: ffffffff814fec10 FS: 00007f87bc0dc780(0000) GS:ffff88803e600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffa0206000 CR3: 0000000010b70000 CR4: 00000000000006e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> bpf_trampoline_update+0x25a/0x6b0 __bpf_trampoline_link_prog+0x101/0x240 bpf_trampoline_link_prog+0x2d/0x50 bpf_tracing_prog_attach+0x24c/0x530 bpf_raw_tp_link_attach+0x73/0x1d0 __sys_bpf+0x100e/0x2570 __x64_sys_bpf+0x1c/0x30 do_syscall_64+0x5b/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd With this patch, when modify_fentry or register_fentry returns -EAGAIN from bpf_tramp_ftrace_ops_func, the pageattr of im->image will be reset to nx+rw.	N/A	More Details
CVE-2022-50655	In the Linux kernel, the following vulnerability has been resolved: ppp: associate skb with a device at tx Syzkaller triggered flow dissector warning with the following: r0 = openat$ppp(0xffffffffffffff9c, &(0x7f0000000000), 0xc0802, 0x0) ioctl$PPPIOCNEWUNIT(r0, 0xc004743e, &(0x7f00000000c0)) ioctl$PPPIOCSACTIVE(r0, 0x40107446, &(0x7f0000000240)={0x2, &(0x7f0000000180)=[{0x20, 0x0, 0x0, 0xfffff034}, {0x6}]}) pwritev(r0, &(0x7f0000000040)=[{&(0x7f0000000140)='\x00!', 0x2}], 0x1, 0x0, 0x0) [9.485814] WARNING: CPU: 3 PID: 329 at net/core/flow_dissector.c:1016 __skb_flow_dissect+0x1ee0/0x1fa0 [9.485929] skb_get_poff+0x53/0xa0 [9.485937] bpf_skb_get_pay_offset+0xe/0x20 [9.485944] ? ppp_send_frame+0xc2/0x5b0 [9.485949] ? _raw_spin_unlock_irqrestore+0x40/0x60 [9.485958] ? __ppp_xmit_process+0x7a/0xe0 [9.485968] ? ppp_xmit_process+0x5b/0xb0 [9.485974] ? ppp_write+0x12a/0x190 [9.485981] ? do_iter_write+0x18e/0x2d0 [9.485987] ? __import_iovec+0x30/0x130 [9.485997] ? do_pwritev+0x1b6/0x240 [9.486016] ? trace_hardirqs_on+0x47/0x50 [9.486023] ? __x64_sys_pwritev+0x24/0x30 [9.486026] ? do_syscall_64+0x3d/0x80 [9.486031] ? entry_SYSCALL_64_after_hwframe+0x63/0xcd Flow dissector tries to find skb net namespace either via device or via socket. Neigher is set in ppp_send_frame, so let's manually use ppp->dev.	N/A	More Details
CVE-2022-50656	In the Linux kernel, the following vulnerability has been resolved: nfc: pn533: Clear nfc_target before being used Fix a slab-out-of-bounds read that occurs in nla_put() called from nfc_genl_send_target() when target->sensb_res_len, which is duplicated from an nfc_target in pn533, is too large as the nfc_target is not properly initialized and retains garbage values. Clear nfc_targets with memset() before they are used. Found by a modified version of syzkaller. BUG: KASAN: slab-out-of-bounds in nla_put Call Trace: memcpy nla_put nfc_genl_dump_targets genl_lock_dumpit netlink_dump __netlink_dump_start genl_family_rcv_msg_dumpit genl_rcv_msg netlink_rcv_skb genl_rcv netlink_unicast netlink_sendmsg sock_sendmsg ____sys_sendmsg ___sys_sendmsg __sys_sendmsg do_syscall_64	N/A	More Details
CVE-2022-50636	In the Linux kernel, the following vulnerability has been resolved: PCI: Fix pci_device_is_present() for VFs by checking PF pci_device_is_present() previously didn't work for VFs because it reads the Vendor and Device ID, which are 0xffff for VFs, which looks like they aren't present. Check the PF instead. Wei Gong reported that if virtio I/O is in progress when the driver is unbound or "0" is written to /sys/.../sriov_numvfs, the virtio I/O operation hangs, which may result in output like this: task:bash state:D stack: 0 pid: 1773 ppid: 1241 flags:0x00004002 Call Trace: schedule+0x4f/0xc0 blk_mq_freeze_queue_wait+0x69/0xa0 blk_mq_freeze_queue+0x1b/0x20 blk_cleanup_queue+0x3d/0xd0 virtblk_remove+0x3c/0xb0 [virtio_blk] virtio_dev_remove+0x4b/0x80 ... device_unregister+0x1b/0x60 unregister_virtio_device+0x18/0x30 virtio_pci_remove+0x41/0x80 pci_device_remove+0x3e/0xb0 This happened because pci_device_is_present(VF) returned "false" in virtio_pci_remove(), so it called virtio_break_device(). The broken vq meant that vring_interrupt() skipped the vq.callback() that would have completed the virtio I/O operation via virtblk_done(). [bhelgaas: commit log, simplify to always use pci_physfn(), add stable tag]	N/A	More Details
CVE-2022-50634	In the Linux kernel, the following vulnerability has been resolved: power: supply: cw2015: Fix potential null-ptr-deref in cw_bat_probe() cw_bat_probe() calls create_singlethread_workqueue() and not checked the ret value, which may return NULL. And a null-ptr-deref may happen: cw_bat_probe() create_singlethread_workqueue() # failed, cw_bat->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-2025-27389	A flaw exists in the verification of application installation sources within ColorOS. Under specific conditions, this issue may cause the risk detection mechanism to fail, which could allow malicious applications to be installed without proper warning.	N/A	More Details
CVE-2025-65230	Barix Instreamer v04.06 and v04.05 contains a stored cross-site scripting (XSS) vulnerability in the Web UI Configuration Streaming Destination input.	N/A	More Details
CVE-2025-63721	HummerRisk thru v1.5.0 is using a vulnerable Snakeyaml component, allowing attackers with normal user privileges to hit the /rule/add API and thereby achieve RCE and take over the server.	N/A	More Details
	Monkeytype is a minimalistic and customizable typing test. In 25.49.0 and earlier, there is improper handling of user input which allows an		

CVE-2025-66563	attacker to execute malicious javascript on anyone viewing a malicious quote submission. quote.text and quote.source are user input, and they're inserted straight into the DOM. If they contain HTML tags, they will be rendered (after some escaping using quotes and textarea tags).	N/A	More Details
CVE-2025-66559	Taiko Alethia is an Ethereum-equivalent, permissionless, based rollup designed to scale Ethereum without compromising its fundamental properties. In 2.3.1 and earlier, TaikoInbox._verifyBatches (packages/protocol/contracts/layer1/based/TaikoInbox.sol:627-678) advanced the local tid to whatever transition matched the current blockHash before knowing whether that batch would actually be verified. When the loop later broke (e.g., cooldown window not yet passed or transition invalidated), the function still wrote that newer tid into batches[lastVerifiedBatchId].verifiedTransitionId after decrementing batchId. Result: the last verified batch could end up pointing at a transition index from the next batch (often zeroed), corrupting the verified chain pointer.	N/A	More Details
CVE-2025-6946	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS allows Stored XSS via the IPS module. This vulnerability requires an authenticated administrator session to a locally managed Firebox. This issue affects Firebox: from 12.0 through 12.11.2.	N/A	More Details
CVE-2025-66509	LaraDashboard is an all-In-one solution to start a Laravel Application. In 2.3.0 and earlier, the password reset flow trusts the Host header, allowing attackers to redirect the administrator’s reset token to an attacker-controlled server. This can be combined with the module installation process to automatically execute the ServiceProvider::boot() method, enabling arbitrary PHP code execution.	N/A	More Details
CVE-2025-65231	Barix Instreamer v04.06 and earlier is vulnerable to Cross Site Scripting (XSS) in the Web UI I/O & Serial configuration page, specifically the CTS close command user-input field which is stored and later rendered on the Status page.	N/A	More Details
CVE-2025-65271	Client-side template injection (CSTI) in Azuriom CMS admin dashboard allows a low-privilege user to execute arbitrary template code in the context of an administrator's session. This can occur via plugins or dashboard components that render untrusted user input, potentially enabling privilege escalation to an administrative account. Fixed in Azuriom 1.2.7.	N/A	More Details
CVE-2025-65548	NUT-14 allows cashu tokens to be created with a preimage hash. However, nutshell (cashubtc/nuts) before 0.18.0 do not validate the size of preimage when the token is spent. The preimage is stored by the mint and attacker can exploit this vulnerability to fill the mint's db nd disk with arbitrary data.	N/A	More Details
CVE-2025-65849	A cryptanalytic break in Altcha Proof-of-Work obfuscation mode version 0.8.0 and later allows for remote visitors to recover the Proof-of-Work nonce in constant time via mathematical deduction.	N/A	More Details
CVE-2025-1910	The WatchGuard Mobile VPN with SSL Client on Windows allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM on the Windows machine where the VPN Client is installed.This issue affects the Mobile VPN with SSL Client 12.0 up to and including 12.11.2.	N/A	More Details
CVE-2022-50633	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: qcom: Fix memory leak in dwc3_qcom_interconnect_init of_icc_get() alloc resources for path handle, we should release it when not need anymore. Like the release in dwc3_qcom_interconnect_exit() function. Add icc_put() in error handling to fix this.	N/A	More Details
CVE-2025-1547	A stack-based buffer overflow vulnerability [CWE-121] in WatchGuard Fireware OS's certificate request command could allow an authenticated privileged user to execute arbitrary code via specially crafted CLI commands.This issue affects Fireware OS: from 12.0 through 12.5.12+701324, from 12.6 through 12.11.2.	N/A	More Details
CVE-2025-1545	An XPath Injection vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to retrieve sensitive information from the Firebox configuration through an exposed authentication or management web interface. This vulnerability only affects Firebox systems that have at least one authentication hotspot configured.This issue affects Fireware OS 11.11 up to and including 11.12.4+541730, 12.0 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-13940	An Expected Behavior Violation [CWE-440] vulnerability in WatchGuard Fireware OS may allow an attacker to bypass the Fireware OS boot time system integrity check and prevent the Firebox from shutting down in the event of a system integrity check failure. The on-demand system integrity check in the Fireware Web UI will correctly show a failed system integrity check message in the event of a failure.This issue affects Fireware OS: from 12.8.1 through 12.11.4, from 2025.1 through 2025.1.2.	N/A	More Details
CVE-2025-65964	n8n is an open source workflow automation platform. Versions 0.123.1 through 1.119.1 do not have adequate protections to prevent RCE through the project's pre-commit hooks. The Add Config operation allows workflows to set arbitrary Git configuration values, including core.hooksPath, which can point to a malicious Git hook that executes arbitrary commands on the n8n host during subsequent Git operations. Exploitation requires the ability to create or modify an n8n workflow using the Git node. This issue is fixed in version 1.119.2. Workarounds include excluding the Git Node (Docs) and avoiding cloning or interacting with untrusted repositories using the Git Node.	N/A	More Details
CVE-2025-13939	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (Gateway Wireless Controller module) allows Stored XSS.This issue affects Fireware OS 11.7.2 up to and including 11.12.4+541730, 12.0 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-66204	WBCE CMS is a content management system. Version 1.6.4 contains a brute-force protection bypass where an attacker can indefinitely reset the counter by modifying `X-Forwarded-For` on each request, gaining unlimited password guessing attempts, effectively bypassing all brute-force protection. The application fully trusts the `X-Forwarded-For` header without validating it or restricting its usage. This issue is fixed in version 1.6.5.	N/A	More Details
CVE-2013-10031	Plack-Middleware-Session versions before 0.17 may be vulnerable to HMAC comparison timing attacks	N/A	More Details
CVE-2022-50631	In the Linux kernel, the following vulnerability has been resolved: RISC-V: kexec: Fix memory leak of fdt buffer This is reported by kmemleak detector: unreferenced object 0xff60000082864000 (size 9588): comm "kexec", pid 146, jiffies 4294900634 (age 64.788s) hex dump (first 32 bytes): d0 0d fe ed 00 00 12 ed 00 00 00 48 00 00 11 40 .....H...@ 00 00 00 28 00 00 00 11 00 00 00 02 00 00 00 00 ...(..... backtrace: [<00000000f95b17c4>] kmemleak_alloc+0x34/0x3e [<00000000b9ec8e3e>] kmalloc_order+0x9c/0xc4 [<00000000a95cf02e>] kmalloc_order_trace+0x34/0xb6 [<00000000f01e68b4>] __kmalloc+0x5c2/0x62a [<000000002bd497b2>] kvmalloc_node+0x66/0xd6 [<00000000906542fa>] of_kexec_alloc_and_setup_fdt+0xa6/0x6ea [<00000000e1166bde>] elf_kexec_load+0x206/0x4ec [<0000000036548e09>] kexec_image_load_default+0x40/0x4c [<0000000079fbe1b4>] sys_kexec_file_load+0x1c4/0x322 [<0000000040c62c03>] ret_from_syscall+0x0/0x2 In elf_kexec_load(), a buffer is allocated via kvmalloc() to store fdt. While it's not freed back to system when kexec kernel is reloaded or unloaded. Then memory leak is caused. Fix it by introducing riscv specific function arch_kimage_file_post_load_cleanup(), and freeing the buffer there.	N/A	More Details

CVE-2022-50632	In the Linux kernel, the following vulnerability has been resolved: drivers: perf: marvell_cn10k: Fix hotplug callback leak in tad_pmu_init() tad_pmu_init() won't remove the callback added by cpuhp_setup_state_multi() when platform_driver_register() failed. Remove the callback by cpuhp_remove_multi_state() in fail path. Similar to the handling of arm_ccn_init() in commit 26242b330093 ("bus: arm-ccn: Prevent hotplug callback leak")	N/A	More Details
CVE-2022-50627	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix monitor mode bringup crash When the interface is brought up in monitor mode, it leads to NULL pointer dereference crash. This crash happens when the packet type is extracted for a SKB. This extraction which is present in the received msdu delivery path,is not needed for the monitor ring packets since they are all RAW packets. Hence appending the flags with "RX_FLAG_ONLY_MONITOR" to skip that extraction. Observed calltrace: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000064 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 CM = 0, WnR = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=0000000048517000 [0000000000000064] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: ath11k_pci ath11k qmi_helpers CPU: 2 PID: 1781 Comm: napi/-271 Not tainted 6.1.0-rc5-wt-ath-656295-gef907406320c-dirty #6 Hardware name: Qualcomm Technologies, Inc. IPQ8074/AP-HK10-C2 (DT) pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : ath11k_hw_qcn9074_rx_desc_get_decap_type+0x34/0x60 [ath11k] lr : ath11k_hw_qcn9074_rx_desc_get_decap_type+0x5c/0x60 [ath11k] sp : ffff80000ef5bb10 x29: ffff80000ef5bb10 x28: 0000000000000000 x27: ffff000007baafa0 x26: ffff000014a91ed0 x25: 0000000000000000 x24: 0000000000000000 x23: ffff800002b77378 x22: ffff000014a91ec0 x21: ffff000006c8d600 x20: 0000000000000000 x19: ffff800002b77740 x18: 0000000000000006 x17: 736564203634343a x16: 656e694c20657079 x15: 0000000000000143 x14: 00000000ffffffea x13: ffff80000ef5b8b8 x12: ffff80000ef5b8c8 x11: ffff80000a591d30 x10: ffff80000a579d40 x9 : c0000000ffffefff x8 : 0000000000000003 x7 : 0000000000017fe8 x6 : ffff80000a579ce8 x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 3a35ec12ed7f8900 x1 : 0000000000000000 x0 : 0000000000000052 Call trace: ath11k_hw_qcn9074_rx_desc_get_decap_type+0x34/0x60 [ath11k] ath11k_dp_rx_deliver_msdu.isra.42+0xa4/0x3d0 [ath11k] ath11k_dp_rx_mon_deliver.isra.43+0x2f8/0x458 [ath11k] ath11k_dp_rx_process_mon_rings+0x310/0x4c0 [ath11k] ath11k_dp_service_srng+0x234/0x338 [ath11k] ath11k_pcic_ext_grp_napi_poll+0x30/0xb8 [ath11k] __napi_poll+0x5c/0x190 napi_threaded_poll+0xf0/0x118 kthread+0xf4/0x110 ret_from_fork+0x10/0x20 Tested-on: QCN9074 hw1.0 PCI WLAN.HK.2.7.0.1-01744-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2022-50625	In the Linux kernel, the following vulnerability has been resolved: serial: amba-pl011: avoid SBSA UART accessing DMACR register Chapter "B Generic UART" in "ARM Server Base System Architecture" [1] documentation describes a generic UART interface. Such generic UART does not support DMA. In current code, sbsa_uart_pops and amba_pl011_pops share the same stop_rx operation, which will invoke pl011_dma_rx_stop, leading to an access of the DMACR register. This commit adds a using_rx_dma check in pl011_dma_rx_stop to avoid the access to DMACR register for SBSA UARTs which does not support DMA. When the kernel enables DMA engine with "CONFIG_DMA_ENGINE=y", Linux SBSA PL011 driver will access PL011 DMACR register in some functions. For most real SBSA Pl011 hardware implementations, the DMACR write behaviour will be ignored. So these DMACR operations will not cause obvious problems. But for some virtual SBSA PL011 hardware, like Xen virtual SBSA PL011 (vpl011) device, the behaviour might be different. Xen vpl011 emulation will inject a data abort to guest, when guest is accessing an unimplemented UART register. As Xen VPL011 is SBSA compatible, it will not implement DMACR register. So when Linux SBSA PL011 driver access DMACR register, it will get an unhandled data abort fault and the application will get a segmentation fault: Unhandled fault at 0xffffffc00944d048 Mem abort info: ESR = 0x96000000 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x00: ttbr address size fault Data abort info: ISV = 0, ISS = 0x00000000 CM = 0, WnR = 0 swapper pgtable: 4k pages, 39-bit VAs, pgdp=0000000020e2e000 [ffffffc00944d048] pgd=100000003ffff803, p4d=100000003ffff803, pud=100000003ffff803, pmd=100000003fffa803, pte=006800009c090f13 Internal error: ttbr address size fault: 96000000 [#1] PREEMPT SMP ... Call trace: pl011_stop_rx+0x70/0x80 tty_port_shutdown+0x7c/0xb4 tty_port_close+0x60/0xcc uart_close+0x34/0x8c tty_release+0x144/0x4c0 __fput+0x78/0x220 ____fput+0x1c/0x30 task_work_run+0x88/0xc0 do_notify_resume+0x8d0/0x123c el0_svc+0xa8/0xc0 el0t_64_sync_handler+0xa4/0x130 el0t_64_sync+0x1a0/0x1a4 Code: b9000083 b901f001 794038a0 8b000042 (b9000041) ---[end trace 83dd93df15c3216f]--- note: bootlogd[132] exited with preempt_count 1 /etc/rcS.d/S07bootlogd: line 47: 132 Segmentation fault start-stop-daemon This has been discussed in the Xen community, and we think it should fix this in Linux. See [2] for more information. [1] https://developer.arm.com/documentation/den0094/c/?lang=en [2] https://lists.xenproject.org/archives/html/xen-devel/2022-11/msg00543.html	N/A	More Details
CVE-2023-53778	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Clean up integer overflow checking in map_user_pages() The encode_dma() function has some validation on in_trans->size but it would be more clear to move those checks to find_and_map_user_pages(). The encode_dma() had two checks: if (in_trans->addr + in_trans->size < in_trans->addr || !in_trans->size) return -EINVAL; The in_trans->addr variable is the starting address. The in_trans->size variable is the total size of the transfer. The transfer can occur in parts and the resources->xferred_dma_size tracks how many bytes we have already transferred. This patch introduces a new variable "remaining" which represents the amount we want to transfer (in_trans->size) minus the amount we have already transferred (resources->xferred_dma_size). I have modified the check for if in_trans->size is zero to instead check if in_trans->size is less than resources->xferred_dma_size. If we have already transferred more bytes than in_trans->size then there are negative bytes remaining which doesn't make sense. If there are zero bytes remaining to be copied, just return success. The check in encode_dma() checked that "addr + size" could not overflow and barring a driver bug that should work, but it's easier to check if we do this in parts. First check that "in_trans->addr + resources->xferred_dma_size" is safe. Then check that "xfer_start_addr + remaining" is safe. My final concern was that we are dealing with u64 values but on 32bit systems the kmalloc() function will truncate the sizes to 32 bits. So I calculated "total = in_trans->size + offset_in_page(xfer_start_addr);" and returned -EINVAL if it were >= SIZE_MAX. This will not affect 64bit systems.	N/A	More Details
CVE-2022-50624	In the Linux kernel, the following vulnerability has been resolved: net: netsec: fix error handling in netsec_register_mdio() If phy_device_register() fails, phy_device_free() need be called to put refcount, so memory of phy device and device name can be freed in callback function. If get_phy_device() fails, mdiobus_unregister() need be called, or it will cause warning in mdiobus_free() and kobject is leaked.	N/A	More Details
CVE-2025-40268	In the Linux kernel, the following vulnerability has been resolved: cifs: client: fix memory leak in smb3_fs_context_parse_param The user calls fsconfig twice, but when the program exits, free() only frees ctx->source for the second fsconfig, not the first. Regarding fc->source, there is no code in the fs context related to its memory reclamation. To fix this memory leak, release the source memory corresponding to ctx or fc before each parsing. syzbot reported: BUG: memory leak unreferenced object 0xffff888128afa360 (size 96): backtrace (crc 79c9c7ba): kstrdup+0x3c/0x80 mm/util.c:84 smb3_fs_context_parse_param+0x229b/0x36c0 fs/smb/client/fs_context.c:1444 BUG: memory leak unreferenced object 0xffff888112c7d900 (size 96): backtrace (crc 79c9c7ba): smb3_fs_context_fullpath+0x70/0x1b0 fs/smb/client/fs_context.c:629 smb3_fs_context_parse_param+0x2266/0x36c0 fs/smb/client/fs_context.c:1438	N/A	More Details
CVE-2025-40269	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix potential overflow of PCM transfer buffer The PCM stream data in USB-audio driver is transferred over USB URB packet buffers, and each packet size is determined dynamically. The packet sizes are limited by some factors such as wMaxPacketSize USB descriptor. OTOH, in the current code, the actually used packet sizes are determined only by the rate and the PPS, which may be bigger than the size limit above. This results in a buffer overflow, as reported by syzbot. Basically when the limit is smaller than the calculated packet size, it implies that something is wrong, most likely a weird USB descriptor. So the best option would be just to return an error at the parameter setup time before doing any further operations. This patch introduces such a sanity check, and returns -EINVAL when the packet size is greater than maxpacksize. The comparison with ep-	N/A	More Details

	>packsize[1] alone should suffice since it's always equal or greater than ep->packsize[0].		
CVE-2025-40270	In the Linux kernel, the following vulnerability has been resolved: mm, swap: fix potential UAF issue for VMA readahead Since commit 78524b05f1a3 ("mm, swap: avoid redundant swap device pinning"), the common helper for allocating and preparing a folio in the swap cache layer no longer tries to get a swap device reference internally, because all callers of __read_swap_cache_async are already holding a swap entry reference. The repeated swap device pinning isn't needed on the same swap device. Caller of VMA readahead is also holding a reference to the target entry's swap device, but VMA readahead walks the page table, so it might encounter swap entries from other devices, and call __read_swap_cache_async on another device without holding a reference to it. So it is possible to cause a UAF when swapoff of device A raced with swapin on device B, and VMA readahead tries to read swap entries from device A. It's not easy to trigger, but in theory, it could cause real issues. Make VMA readahead try to get the device reference first if the swap device is a different one from the target entry.	N/A	More Details
CVE-2025-40271	In the Linux kernel, the following vulnerability has been resolved: fs/proc: fix uaf in proc_readdir_de() Pde is erased from subdir rbtree through rb_erase(), but not set the node to EMPTY, which may result in uaf access. We should use RB_CLEAR_NODE() set the erased node to EMPTY, then pde_subdir_next() will return NULL to avoid uaf access. We found an uaf issue while using stress-ng testing, need to run testcase getdent and tun in the same time. The steps of the issue is as follows: 1) use getdent to traverse dir /proc/pid/net/dev_snmp6/, and current pde is tun3; 2) in the [time windows] unregister netdevice tun3 and tun2, and erase them from rbtree. erase tun3 first, and then erase tun2. the pde(tun2) will be released to slab; 3) continue to getdent process, then pde_subdir_next() will return pde(tun2) which is released, it will case uaf access. CPU 0 | CPU 1 ---------- traverse dir /proc/pid/net/dev_snmp6/ | unregister_netdevice(tun->dev) //tun3 tun2 sys_getdents64() | iterate_dir() | proc_readdir() | proc_readdir_de() | snmp6_unregister_dev() pde_get(de); | proc_remove() read_unlock(&proc_subdir_lock); | remove_proc_subtree() | write_lock(&proc_subdir_lock); [time window] | rb_erase(&root->subdir_node, &parent->subdir); | write_unlock(&proc_subdir_lock); read_lock(&proc_subdir_lock); | next = pde_subdir_next(de); | pde_put(de); | de = next; //UAF | rbtree of dev_snmp6 | pde(tun3) / \ NULL pde(tun2)	N/A	More Details
CVE-2025-40272	In the Linux kernel, the following vulnerability has been resolved: mm/secretmem: fix use-after-free race in fault handler When a page fault occurs in a secret memory file created with `memfd_secret(2)`, the kernel will allocate a new folio for it, mark the underlying page as not-present in the direct map, and add it to the file mapping. If two tasks cause a fault in the same page concurrently, both could end up allocating a folio and removing the page from the direct map, but only one would succeed in adding the folio to the file mapping. The task that failed undoes the effects of its attempt by (a) freeing the folio again and (b) putting the page back into the direct map. However, by doing these two operations in this order, the page becomes available to the allocator again before it is placed back in the direct mapping. If another task attempts to allocate the page between (a) and (b), and the kernel tries to access it via the direct map, it would result in a supervisor not-present page fault. Fix the ordering to restore the direct map before the folio is freed.	N/A	More Details
CVE-2025-40273	In the Linux kernel, the following vulnerability has been resolved: NFSD: free copynotify stateid in nfs4_free_ol_stateid() Typically copynotify stateid is freed either when parent's stateid is being close/freed or in nfsd4_laundromat if the stateid hasn't been used in a lease period. However, in case when the server got an OPEN (which created a parent stateid), followed by a COPY_NOTIFY using that stateid, followed by a client reboot. New client instance while doing CREATE_SESSION would force expire previous state of this client. It leads to the open state being freed thru release_openowner-> nfs4_free_ol_stateid() and it finds that it still has copynotify stateid associated with it. We currently print a warning and is triggerred WARNING: CPU: 1 PID: 8858 at fs/nfsd/nfs4state.c:1550 nfs4_free_ol_stateid+0xb0/0x100 [nfsd] This patch, instead, frees the associated copynotify stateid here. If the parent stateid is freed (without freeing the copynotify stateids associated with it), it leads to the list corruption when laundromat ends up freeing the copynotify state later. [1626.839430] Internal error: Oops - BUG: 00000000f2000800 [#1] SMP [1626.842828] Modules linked in: nfnetlink_queue nfnetlink_log bluetooth cfg80211 rpcrdma rdma_cm iw_cm ib_cm ib_core nfsd nfs_acl lockd grace nfs_localio ext4 crc16 mbcache jbd2 overlay uinput snd_seq_dummy snd_hrtimer qrtr rfkill vfat fat uvcvideo snd_hda_codec_generic videobuf2_vmalloc videobuf2_memops snd_hda_intel uvc snd_intel_dspcfg videobuf2_v4l2 videobuf2_common snd_hda_codec snd_hda_core videodev snd_hwdep snd_seq mc snd_seq_device snd_pcm snd_timer snd soundcore sg loop auth_rpcgss vsock_loopback vmw_vsock_virtio_transport_common vmw_vsock_vmci_transport vmw_vmci vsock xfs 8021q garp stp llc mrp nvme ghash_ce e1000e nvme_core sr_mod nvme_keyring nvme_auth cdrom vmwgfx drm_ttm_helper ttm sunrpc dm_mirror dm_region_hash dm_log iscsi_tcp libiscsi_tcp libiscsi scsi_transport_iscsi fuse dm_multipath dm_mod nfnetlink [1626.855594] CPU: 2 UID: 0 PID: 199 Comm: kworker/u24:33 Kdump: loaded Tainted: G B W 6.17.0-rc7+ #22 PREEMPT(voluntary) [1626.857075] Tainted: [B]=BAD_PAGE, [W]=WARN [1626.857573] Hardware name: VMware, Inc. VMware20,1/VBSA, BIOS VMW201.00V.24006586.BA64.2406042154 06/04/2024 [1626.858724] Workqueue: nfsd4 laundromat_main [nfsd] [1626.859304] pstate: 61400005 (nZCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) [1626.860010] pc : __list_del_entry_valid_or_report+0x148/0x200 [1626.860601] lr : __list_del_entry_valid_or_report+0x148/0x200 [1626.861182] sp : ffff8000881d7a40 [1626.861521] x29: ffff8000881d7a40 x28: 0000000000000018 x27: ffff0000c2a98200 [1626.862260] x26: 0000000000000600 x25: 0000000000000000 x24: ffff8000881d7b20 [1626.862986] x23: ffff0000c2a981e8 x22: 1fffe00012410e7d x21: ffff0000920873e8 [1626.863701] x20: ffff0000920873e8 x19: ffff000086f22998 x18: 0000000000000000 [1626.864421] x17: 20747562202c3839 x16: 3932326636383030 x15: 3030666666662065 [1626.865092] x14: 6220646c756f6873 x13: 0000000000000001 x12: ffff60004fd9e4a3 [1626.865713] x11: 1fffe0004fd9e4a2 x10: ffff60004fd9e4a2 x9 : dfff800000000000 [1626.866320] x8 : 00009fffb0261b5e x7 : ffff00027ecf2513 x6 : 0000000000000001 [1626.866938] x5 : ffff00027ecf2510 x4 : ffff60004fd9e4a3 x3 : 0000000000000000 [1626.867553] x2 : 0000000000000000 x1 : ffff000096069640 x0 : 000000000000006d [1626.868167] Call trace: [1626.868382] __list_del_entry_valid_or_report+0x148/0x200 (P) [1626.868876] _free_cpntf_state_locked+0xd0/0x268 [nfsd] [1626.869368] nfs4_laundromat+0x6f8/0x1058 [nfsd] [1626.869813] laundromat_main+0x24/0x60 [nfsd] [1626.870231] process_one_work+0x584/0x1050 [1626.870595] worker_thread+0x4c4/0xc60 [1626.870893] kthread+0x2f8/0x398 [1626.871146] ret_from_fork+0x10/0x20 [1626.871422] Code: aa1303e1 aa1403e3 910e8000 97bc55d7 (d4210000) [1626.871892] SMP: stopping secondary CPUs	N/A	More Details
CVE-2025-40274	In the Linux kernel, the following vulnerability has been resolved: KVM: guest_memfd: Remove bindings on memslot deletion when gmem is dying When unbinding a memslot from a guest_memfd instance, remove the bindings even if the guest_memfd file is dying, i.e. even if its file refcount has gone to zero. If the memslot is freed before the file is fully released, nullifying the memslot side of the binding in kvm_gmem_release() will write to freed memory, as detected by syzbot+KASAN: == BUG: KASAN: slab-use-after-free in kvm_gmem_release+0x176/0x440 virt/kvm/guest_memfd.c:353 Write of size 8 at addr ffff88807befa508 by task syz.0.17/6022 CPU: 0 UID: 0 PID: 6022 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/02/2025 Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 kvm_gmem_release+0x176/0x440 virt/kvm/guest_memfd.c:353 __fput+0x44c/0xa70 fs/file_table.c:468 task_work_run+0x1d4/0x260 kernel/task_work.c:227 resume_user_mode_work include/linux/resume_user_mode.h:50 [inline] exit_to_user_mode_loop+0xe9/0x130 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+0x2bd/0xfa0 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fbeeff8efc9 </TASK> Allocated by task 6023: kasan_save_stack mm/kasan/common.c:56 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:77 poison_kmalloc_redzone mm/kasan/common.c:397 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:414 kasan_kmalloc include/linux/kasan.h:262 [inline] __kmalloc_cache_noprof+0x3e2/0x700 mm/slub.c:5758 kmalloc_noprof include/linux/slab.h:957 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] kvm_set_memory_region+0x747/0xb90	N/A	More Details

	virt/kvm/kvm_main.c:2104 kvm_vm_ioctl_set_memory_region+0x6f/0xd0 virt/kvm/kvm_main.c:2154 kvm_vm_ioctl+0x957/0xc60 virt/kvm/kvm_main.c:5201 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 6023: kasan_save_stack mm/kasan/common.c:56 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:77 kasan_save_free_info+0x46/0x50 mm/kasan/generic.c:584 poison_slab_object mm/kasan/common.c:252 [inline] __kasan_slab_free+0x5c/0x80 mm/kasan/common.c:284 kasan_slab_free include/linux/kasan.h:234 [inline] slab_free_hook mm/slub.c:2533 [inline] slab_free mm/slub.c:6622 [inline] kfree+0x19a/0x6d0 mm/slub.c:6829 kvm_set_memory_region+0x9c4/0xb90 virt/kvm/kvm_main.c:2130 kvm_vm_ioctl_set_memory_region+0x6f/0xd0 virt/kvm/kvm_main.c:2154 kvm_vm_ioctl+0x957/0xc60 virt/kvm/kvm_main.c:5201 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Deliberately don't acquire filemap invalid lock when the file is dying as the lifecycle of f_mapping is outside the purview of KVM. Dereferencing the mapping is *probably* fine, but there's no need to invalidate anything as memslot deletion is responsible for zapping SPTEs, and the only code that can access the dying file is kvm_gmem_release(), whose core code is mutual ---truncated---		
CVE-2025-40275	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix NULL pointer dereference in snd_usb_mixer_controls_badd In snd_usb_create_streams(), for UAC version 3 devices, the Interface Association Descriptor (IAD) is retrieved via usb_ifnum_to_if(). If this call fails, a fallback routine attempts to obtain the IAD from the next interface and sets a BADD profile. However, snd_usb_mixer_controls_badd() assumes that the IAD retrieved from usb_ifnum_to_if() is always valid, without performing a NULL check. This can lead to a NULL pointer dereference when usb_ifnum_to_if() fails to find the interface descriptor. This patch adds a NULL pointer check after calling usb_ifnum_to_if() in snd_usb_mixer_controls_badd() to prevent the dereference. This issue was discovered by syzkaller, which triggered the bug by sending a crafted USB device descriptor.	N/A	More Details
CVE-2025-40276	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Flush shmem writes before mapping buffers CPU-uncached The shmem layer zeroes out the new pages using cached mappings, and if we don't CPU-flush we might leave dirty cachelines behind, leading to potential data leaks and/or asynchronous buffer corruption when dirty cachelines are evicted.	N/A	More Details
CVE-2025-40277	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Validate command header size against SVGA_CMD_MAX_DATASIZE This data originates from userspace and is used in buffer offset calculations which could potentially overflow causing an out-of-bounds access.	N/A	More Details
CVE-2025-40278	In the Linux kernel, the following vulnerability has been resolved: net: sched: act_ife: initialize struct tc_ife to fix KMSAN kernel-infoleak Fix a KMSAN kernel-infoleak detected by the syzbot . [net?] KMSAN: kernel-infoleak in __skb_datagram_iter In tcf_ife_dump(), the variable 'opt' was partially initialized using a designatied initializer. While the padding bytes are reamined uninitialized. nla_put() copies the entire structure into a netlink message, these uninitialized bytes leaked to userspace. Initialize the structure with memset before assigning its fields to ensure all members and padding are cleared prior to beign copied. This change silences the KMSAN report and prevents potential information leaks from the kernel memory. This fix has been tested and validated by syzbot. This patch closes the bug reported at the following syzkaller link and ensures no infoleak.	N/A	More Details
CVE-2025-40279	In the Linux kernel, the following vulnerability has been resolved: net: sched: act_connmark: initialize struct tc_ife to fix kernel leak In tcf_connmark_dump(), the variable 'opt' was partially initialized using a designatied initializer. While the padding bytes are reamined uninitialized. nla_put() copies the entire structure into a netlink message, these uninitialized bytes leaked to userspace. Initialize the structure with memset before assigning its fields to ensure all members and padding are cleared prior to beign copied.	N/A	More Details
CVE-2025-40280	In the Linux kernel, the following vulnerability has been resolved: tipc: Fix use-after-free in tipc_mon_reinit_self(). syzbot reported use-after-free of tipc_net(net)->monitors[] in tipc_mon_reinit_self(). [0] The array is protected by RTNL, but tipc_mon_reinit_self() iterates over it without RTNL. tipc_mon_reinit_self() is called from tipc_net_finalize(), which is always under RTNL except for tipc_net_finalize_work(). Let's hold RTNL in tipc_net_finalize_work(). [0]: BUG: KASAN: slab-use-after-free in __raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:110 [inline] BUG: KASAN: slab-use-after-free in _raw_spin_lock_irqsave+0xa7/0xf0 kernel/locking/spinlock.c:162 Read of size 1 at addr ffff88805eae1030 by task kworker/0:7/5989 CPU: 0 UID: 0 PID: 5989 Comm: kworker/0:7 Not tainted syzkaller #0 PREEMPT_{RT,(full)} Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/18/2025 Workqueue: events tipc_net_finalize_work Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 __kasan_check_byte+0x2a/0x40 mm/kasan/common.c:568 kasan_check_byte include/linux/kasan.h:399 [inline] lock_acquire+0x8d/0x360 kernel/locking/lockdep.c:5842 __raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:110 [inline] _raw_spin_lock_irqsave+0xa7/0xf0 kernel/locking/spinlock.c:162 rtlock_slowlock kernel/locking/rtmutex.c:1894 [inline] rwbase_rtmutex_lock_state kernel/locking/spinlock_rt.c:160 [inline] rwbase_write_lock+0xd3/0x7e0 kernel/locking/rwbase_rt.c:244 rt_write_lock+0x76/0x110 kernel/locking/spinlock_rt.c:243 write_lock_bh include/linux/rwlock_rt.h:99 [inline] tipc_mon_reinit_self+0x79/0x430 net/tipc/monitor.c:718 tipc_net_finalize+0x115/0x190 net/tipc/net.c:140 process_one_work kernel/workqueue.c:3236 [inline] process_scheduled_works+0xade/0x17b0 kernel/workqueue.c:3319 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3400 kthread+0x70e/0x8a0 kernel/kthread.c:463 ret_from_fork+0x439/0x7d0 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> Allocated by task 6089: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:388 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:405 kasan_kmalloc include/linux/kasan.h:260 [inline] __kmalloc_cache_noprof+0x1a8/0x320 mm/slub.c:4407 kmalloc_noprof include/linux/slab.h:905 [inline] kzalloc_noprof include/linux/slab.h:1039 [inline] tipc_mon_create+0xc3/0x4d0 net/tipc/monitor.c:657 tipc_enable_bearer net/tipc/bearer.c:357 [inline] __tipc_nl_bearer_enable+0xe16/0x13f0 net/tipc/bearer.c:1047 __tipc_nl_compat_doit net/tipc/netlink_compat.c:371 [inline] tipc_nl_compat_doit+0x3bc/0x5f0 net/tipc/netlink_compat.c:393 tipc_nl_compat_handle net/tipc/netlink_compat.c:-1 [inline] tipc_nl_compat_recv+0x83c/0xbe0 net/tipc/netlink_compat.c:1321 genl_family_rcv_msg_doit+0x215/0x300 net/netlink/genetlink.c:1115 genl_family_rcv_msg net/netlink/genetlink.c:1195 [inline] genl_rcv_msg+0x60e/0x790 net/netlink/genetlink.c:1210 netlink_rcv_skb+0x208/0x470 net/netlink/af_netlink.c:2552 genl_rcv+0x28/0x40 net/netlink/genetlink.c:1219 netlink_unicast_kernel net/netlink/af_netlink.c:1320 [inline] netlink_unicast+0x846/0xa10 net/netlink/af_netlink.c:1346 netlink_sendmsg+0x805/0xb30 net/netlink/af_netlink.c:1896 sock_sendmsg_nosec net/socket.c:714 [inline] __sock_sendmsg+0x21c/0x270 net/socket.c:729 ____sys_sendmsg+0x508/0x820 net/socket.c:2614 ___sys_sendmsg+0x21f/0x2a0 net/socket.c:2668 __sys_sendmsg net/socket.c:2700 [inline] __do_sys_sendmsg net/socket.c:2705 [inline] __se_sys_sendmsg net/socket.c:2703 [inline] __x64_sys_sendmsg+0x1a1/0x260 net/socket.c:2703 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/ ---truncated---	N/A	More Details
CVE-2025-40281	In the Linux kernel, the following vulnerability has been resolved: sctp: prevent possible shift-out-of-bounds in sctp_transport_update_rto syzbot reported a possible shift-out-of-bounds [1] Blamed commit added rto_alpha_max and rto_beta_max set to 1000. It is unclear if some sctp users are setting very large rto_alpha and/or rto_beta. In order to prevent user regression, perform the test at run time. Also add READ_ONCE() annotations as sysctl values can change under us. [1] UBSAN: shift-out-of-bounds in net/sctp/transport.c:509:41 shift exponent 64 is too large for 32-bit type 'unsigned int' CPU: 0 UID: 0 PID: 16704 Comm: syz.2.2320 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/02/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x16c/0x1f0 lib/dump_stack.c:120 ubsan_epilogue lib/ubsan.c:233 [inline] __ubsan_handle_shift_out_of_bounds+0x27f/0x420 lib/ubsan.c:494 sctp_transport_update_rto.cold+0x1c/0x34b net/sctp/transport.c:509	N/A	More Details

	sctp_check_transmitted+0x11c4/0x1c30 net/sctp/outqueue.c:1502 sctp_outq_sack+0x4ef/0x1b20 net/sctp/outqueue.c:1338 sctp_cmd_process_sack net/sctp/sm_sideeffect.c:840 [inline] sctp_cmd_interpreter net/sctp/sm_sideeffect.c:1372 [inline]		
CVE-2025-40282	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: 6lowpan: reset link-local header on ipv6 recv path Bluetooth 6lowpan.c netdev has header_ops, so it must set link-local header for RX skb, otherwise things crash, eg. with AF_PACKET SOCK_RAW Add missing skb_reset_mac_header() for uncompressed ipv6 RX path. For the compressed one, it is done in lowpan_header_decompress(). Log: (BlueZ 6lowpan-tester Client Recv Raw - Success) ------ kernel BUG at net/core/skbuff.c:212! Call Trace: <IRQ> ... packet_rcv (net/packet/af_packet.c:2152) ... <TASK> __local_bh_enable_ip (kernel/softirq.c:407) netif_rx (net/core/dev.c:5648) chan_recv_cb (net/bluetooth/6lowpan.c:294 net/bluetooth/6lowpan.c:359) ------	N/A	More Details
CVE-2025-40283	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: reorder cleanup in btusb_disconnect to avoid UAF There is a KASAN: slab-use-after-free read in btusb_disconnect(). Calling "usb_driver_release_interface(&btusb_driver, data->intf)" will free the btusb data associated with the interface. The same data is then used later in the function, hence the UAF. Fix by moving the accesses to btusb data to before the data is free'd.	N/A	More Details
CVE-2025-40284	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: cancel mesh send timer when hdev removed mesh_send_done timer is not canceled when hdev is removed, which causes crash if the timer triggers after hdev is gone. Cancel the timer when MGMT removes the hdev, like other MGMT timers. Should fix the BUG: sporadically seen by BlueZ test bot (in "Mesh - Send cancel - 1" test). Log: ------ BUG: KASAN: slab-use-after-free in run_timer_softirq+0x76b/0x7d0 ... Freed by task 36: kasan_save_stack+0x24/0x50 kasan_save_track+0x14/0x30 __kasan_save_free_info+0x3a/0x60 __kasan_slab_free+0x43/0x70 kfree+0x103/0x500 device_release+0x9a/0x210 kobject_put+0x100/0x1e0 vhci_release+0x18b/0x240 ------	N/A	More Details
CVE-2025-40285	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix possible refcount leak in smb2_sess_setup() Reference count of ksmbd_session will leak when session need reconnect. Fix this by adding the missing ksmbd_user_session_put().	N/A	More Details
CVE-2025-40286	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix possible memory leak in smb2_read() Memory leak occurs when ksmbd_vfs_read() fails. Fix this by adding the missing kvfree().	N/A	More Details
CVE-2025-40287	In the Linux kernel, the following vulnerability has been resolved: exfat: fix improper check of dentry.stream.valid_size We found an infinite loop bug in the exFAT file system that can lead to a Denial-of-Service (DoS) condition. When a dentry in an exFAT filesystem is malformed, the following system calls — SYS_openat, SYS_ftruncate, and SYS_pwrite64 — can cause the kernel to hang. Root cause analysis shows that the size validation code in exfat_find() does not check whether dentry.stream.valid_size is negative. As a result, the system calls mentioned above can succeed and eventually trigger the DoS issue. This patch adds a check for negative dentry.stream.valid_size to prevent this vulnerability.	N/A	More Details
CVE-2025-40288	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix NULL pointer dereference in VRAM logic for APU devices Previously, APU platforms (and other scenarios with uninitialized VRAM managers) triggered a NULL pointer dereference in `ttm_resource_manager_usage()`. The root cause is not that the `struct ttm_resource_manager *man` pointer itself is NULL, but that `man->bdev` (the backing device pointer within the manager) remains uninitialized (NULL) on APUs—since APUs lack dedicated VRAM and do not fully set up VRAM manager structures. When `ttm_resource_manager_usage()` attempts to acquire `man->bdev->lru_lock`, it dereferences the NULL `man->bdev`, leading to a kernel OOPS. 1. **amdgpu_cs.c**: Extend the existing bandwidth control check in `amdgpu_cs_get_threshold_for_moves()` to include a check for `ttm_resource_manager_used()`. If the manager is not used (uninitialized `bdev`), return 0 for migration thresholds immediately—skipping VRAM-specific logic that would trigger the NULL dereference. 2. **amdgpu_kms.c**: Update the `AMDGPU_INFO_VRAM_USAGE` ioctl and memory info reporting to use a conditional: if the manager is used, return the real VRAM usage; otherwise, return 0. This avoids accessing `man->bdev` when it is NULL. 3. **amdgpu_virt.c**: Modify the vf2pf (virtual function to physical function) data write path. Use `ttm_resource_manager_used()` to check validity: if the manager is usable, calculate `fb_usage` from VRAM usage; otherwise, set `fb_usage` to 0 (APUs have no discrete framebuffer to report). This approach is more robust than APU-specific checks because it: - Works for all scenarios where the VRAM manager is uninitialized (not just APUs), - Aligns with TTM's design by using its native helper function, - Preserves correct behavior for discrete GPUs (which have fully initialized `man->bdev` and pass the `ttm_resource_manager_used()` check). v4: use ttm_resource_manager_used(&adev->mman.vram_mgr.manager) instead of checking the adev->gmc.is_app_apu flag (Christian)	N/A	More Details
CVE-2025-40267	In the Linux kernel, the following vulnerability has been resolved: io_uring/rw: ensure allocated iovec gets cleared for early failure A previous commit reused the recyling infrastructure for early cleanup, but this is not enough for the case where our internal caches have overflowed. If this happens, then the allocated iovec can get leaked if the request is also aborted early. Reinstate the previous forced free of the iovec for that situation.	N/A	More Details
CVE-2020-36876	ReQuest Serious Play F3 Media Server versions 7.0.3.4968 (Pro), 7.0.2.4954, 6.5.2.4954, 6.4.2.4681, 6.3.2.4203, and 2.0.1.823 allows unauthenticated attackers to disclose the webserver's Python debug log file containing system information, credentials, paths, processes and command arguments running on the device. Attackers can access sensitive information by visiting the message_log page.	N/A	More Details
CVE-2020-36877	ReQuest Serious Play F3 Media Server 7.0.3 contains an unauthenticated remote code execution vulnerability that allows attackers to execute arbitrary commands as the web server user. Attackers can upload PHP executable files via the Quick File Uploader page, resulting in remote code execution on the server.	N/A	More Details
CVE-2025-34262	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/devices/name/{agent_id} endpoint. When an authenticated user renames a device, the new_name value is stored and later rendered in device listings or detail views without proper HTML sanitation. An attacker can inject malicious script into the device name, which is then executed in the browser context of users who view or interact with the affected device, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-66566	yawkat LZ4 Java provides LZ4 compression for Java. Insufficient clearing of the output buffer in Java-based decompressor implementations in lz4-java 1.10.0 and earlier allows remote attackers to read previous buffer contents via crafted compressed input. In applications where the output buffer is reused without being cleared, this may lead to disclosure of sensitive data. JNI-based implementations are not affected. This vulnerability is fixed in 1.10.1.	N/A	More Details
CVE-2025-66581	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to 2.41.0, a flaw in the server-side authorization logic allowed authenticated users to perform actions beyond their assigned roles across multiple features. Because the affected endpoints relied on client-side or UI-level checks instead of enforcing permissions on the server, users with low-privileged roles (such as students) could perform operations intended only for instructors or administrators via directly using the API's. This vulnerability is fixed in 2.41.0.	N/A	More Details
CVE-2025-	A vulnerability exists in Google Apigee's JavaCallout policy https://docs.apigee.com/api-platform/reference/policies/java-callout-policy that allows for remote code execution. It is possible for a user to write a JavaCallout that injected a malicious object into the MessageContext to execute arbitrary Java code and system commands at runtime, leading to unauthorized access to data, lateral movement within the	N/A	More

13426	network, and access to backend systems. The Apigee hybrid versions below have all been updated to protect from this vulnerability: * Hybrid_1.11.2+ * Hybrid_1.12.4+ * Hybrid_1.13.3+ * Hybrid_1.14.1+ * OPDK_5202+ * OPDK_5300+		Details
CVE-2025-34291	Langflow versions up to and including 1.6.9 contain a chained vulnerability that enables account takeover and remote code execution. An overly permissive CORS configuration (allow_origins='*' with allow_credentials=True) combined with a refresh token cookie configured as SameSite=None allows a malicious webpage to perform cross-origin requests that include credentials and successfully call the refresh endpoint. An attacker-controlled origin can therefore obtain fresh access_token / refresh_token pairs for a victim session. Obtained tokens permit access to authenticated endpoints — including built-in code-execution functionality — allowing the attacker to execute arbitrary code and achieve full system compromise.	N/A	More Details
CVE-2025-13292	A vulnerability in Apigee-X allowed an attacker to gain unauthorized read and write access to Apigee Analytics (AX) data and access logs belonging to other Apigee customer organizations. Apigee-X was found to be vulnerable. This vulnerability was patched in version 1-16-0-apigee-3. No user action is required for this.	N/A	More Details
CVE-2025-34266	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/plugin-config/addins/menus endpoint. When an authenticated user adds or edits an AddIns menu entry, the label and path values are stored in plugin configuration data and later rendered in the AddIns UI without proper HTML sanitation. An attacker can inject malicious script into either field, which is then executed in the browser context of users who view or interact with the affected AddIns entry, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34265	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/rule-engines endpoint. When an authenticated user creates or updates a rule for an agent, the rule fields min, max, and unit are stored and later rendered in rule listings or detail views without proper HTML sanitation. An attacker can inject malicious script into one or more of these fields, which is then executed in the browser context of users who view or interact with the affected rule, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34264	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/dog/{agentId} endpoint. When an authenticated user adds or edits Software Watchdog process rules for an agent, the monitored process name is stored in the settings array and later rendered in the Software Watchdog UI without proper HTML sanitation. An attacker can inject malicious script into the process name, which is then executed in the browser context of users who view or interact with the affected rules, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34263	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/plugin-config/dashboards/menus endpoint. When an authenticated user adds or edits a dashboard entry, the label and path values are stored in plugin configuration data and later rendered in the dashboard UI without proper HTML sanitation. An attacker can inject malicious script into either field, which is then executed in the browser context of users who view or interact with the affected dashboard, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34261	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/devicegroups/ endpoint. When an authenticated user creates a device group, the name and description values are stored and later rendered in device group listings without proper HTML sanitation. An attacker can inject malicious script into either field, which is then executed in the browser context of users who view or interact with the affected device group, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2020-36878	ReQuest Serious Play Media Player 3.0 contains an unauthenticated file disclosure vulnerability when input passed through the 'file' parameter in and script is not properly verified before being used to read web log files. Attackers can exploit this to disclose contents of files from local resources.	N/A	More Details
CVE-2025-34260	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/action/schedule endpoint. When an authenticated user adds a schedule to an existing task, the schedule name is stored and later rendered in schedule listings without HTML sanitation. An attacker can inject malicious script into the schedule name, which is then executed in the browser context of users who view or interact with the affected schedule, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34259	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/devicemap/building endpoint. When an authenticated user creates a map entry, the name parameter is stored and later rendered in the map list UI without HTML sanitzation. An attacker can inject malicious script into the map entry name, which is then executed in the browser context of users who view or interact with the affected map entry, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34258	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/devicemap/plan endpoint. When an authenticated user adds an area to a map entry, the name parameter is stored and later rendered in the map list without HTML sanitization. An attacker can inject malicious script into the area name, which is then executed in the browser context of users who view or interact with the affected map entry, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34257	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a stored cross-site scripting (XSS) vulnerability in the /rmm/v1/action/defined endpoint. When an authenticated user creates a task, the defined_name value is stored and later rendered in the Overview page without HTML sanitization. An attacker can inject malicious script into defined_name, which is then executed in the browser context of users who view the affected task, potentially enabling session compromise and unauthorized actions as the victim.	N/A	More Details
CVE-2025-34256	Advantech WISE-DeviceOn Server versions prior to 5.4 contain a hard-coded cryptographic key vulnerability. The product uses a static HS512 HMAC secret for signing EIRMMToken JWTs across all installations. The server accepts forged JWTs that need only contain a valid email claim, allowing a remote unauthenticated attacker to generate arbitrary tokens and impersonate any DeviceOn account, including the root super admin. Successful exploitation permits full administrative control of the DeviceOn instance and can be leveraged to execute code on managed agents through DeviceOn's remote management features.	N/A	More Details
CVE-2020-36882	Flexsense DiskBoss 7.7.14 allows unauthenticated attackers to upload arbitrary files via /Command/Search Files/Directory field, leading to a denial of service by crashing the application.	N/A	More Details
CVE-2020-36881	Flexsense DiskBoss 7.7.14 contains a local buffer overflow vulnerability in the 'Input Directory' component that allows unauthenticated attackers to execute arbitrary code on the system. Attackers can exploit this by pasting a specially crafted directory path into the 'Add Input Directory' field.	N/A	More Details
CVE-	Flexsense DiskBoss 7.7.14 contains a local buffer overflow vulnerability in the 'Reports and Data Directory' field that allows an attacker to		More

2020-36880	execute arbitrary code on the system.	N/A	Details
CVE-2020-36879	Flexsense DiskBoss 11.7.28 allows unauthenticated attackers to elevate their privileges using any of its services, enabling remote code execution during startup or reboot with escalated privileges. Attackers can exploit the unquoted service path vulnerability by specifying a malicious service name in the 'sc qc' command, allowing them to execute arbitrary system commands.	N/A	More Details
CVE-2025-40289	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: hide VRAM sysfs attributes on GPUs without VRAM Otherwise accessing them can cause a crash.	N/A	More Details
CVE-2025-66471	urllib3 is a user-friendly HTTP client library for Python. Starting in version 1.0 and prior to 2.6.0, the Streaming API improperly handles highly compressed data. urllib3's streaming API is designed for the efficient handling of large HTTP responses by reading the content in chunks, rather than loading the entire response body into memory at once. When streaming a compressed response, urllib3 can perform decoding or decompression based on the HTTP Content-Encoding header (e.g., gzip, deflate, br, or zstd). The library must read compressed data from the network and decompress it until the requested chunk size is met. Any resulting decompressed data that exceeds the requested amount is held in an internal buffer for the next read operation. The decompression logic could cause urllib3 to fully decode a small amount of highly compressed data in a single operation. This can result in excessive resource consumption (high CPU usage and massive memory allocation for the decompressed data.	N/A	More Details
CVE-2025-40290	In the Linux kernel, the following vulnerability has been resolved: xsk: avoid data corruption on cq descriptor number Since commit 30f241fcf52a ("xsk: Fix immature cq descriptor production"), the descriptor number is stored in skb control block and xsk_cq_submit_addr_locked() relies on it to put the umem addrs onto pool's completion queue. skb control block shouldn't be used for this purpose as after transmit xsk doesn't have control over it and other subsystems could use it. This leads to the following kernel panic due to a NULL pointer dereference. BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 2 UID: 1 PID: 927 Comm: p4xsk.bin Not tainted 6.16.12+deb14-cloud-amd64 #1 PREEMPT(lazy) Debian 6.16.12-1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-debian-1.17.0-1 04/01/2014 RIP: 0010:xsk_destruct_skb+0xd0/0x180 [...] Call Trace: <IRQ> ? napi_complete_done+0x7a/0x1a0 ip_rcv_core+0x1bb/0x340 ip_rcv+0x30/0x1f0 __netif_receive_skb_one_core+0x85/0xa0 process_backlog+0x87/0x130 __napi_poll+0x28/0x180 net_rx_action+0x339/0x420 handle_softirqs+0xdc/0x320 ? handle_edge_irq+0x90/0x1e0 do_softirq.part.0+0x3b/0x60 </IRQ> <TASK> __local_bh_enable_ip+0x60/0x70 __dev_direct_xmit+0x14e/0x1f0 __xsk_generic_xmit+0x482/0xb70 ? __remove_hrtimer+0x41/0xa0 ? __xsk_generic_xmit+0x51/0xb70 ? _raw_spin_unlock_irqrestore+0xe/0x40 xsk_sendmsg+0xda/0x1c0 __sys_sendto+0x1ee/0x200 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x84/0x2f0 ? __pfx_pollwake+0x10/0x10 ? __rseq_handle_notify_resume+0xad/0x4c0 ? restore_fpregs_from_fpstate+0x3c/0x90 ? switch_fpu_return+0x5b/0xe0 ? do_syscall_64+0x204/0x2f0 ? do_syscall_64+0x204/0x2f0 ? do_syscall_64+0x204/0x2f0 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> [...] Kernel panic - not syncing: Fatal exception in interrupt Kernel Offset: 0x1c000000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff) Instead use the skb destructor_arg pointer along with pointer tagging. As pointers are always aligned to 8B, use the bottom bit to indicate whether this a single address or an allocated struct containing several addresses.	N/A	More Details
CVE-2022-50583	In the Linux kernel, the following vulnerability has been resolved: md/raid0, raid10: Don't set discard sectors for request queue It should use disk_stack_limits to get a proper max_discard_sectors rather than setting a value by stack drivers. And there is a bug. If all member disks are rotational devices, raid0/raid10 set max_discard_sectors. So the member devices are not ssd/nvme, but raid0/raid10 export the wrong value. It reports warning messages in function __blkdev_issue_discard when mkfs.xfs like this: [4616.022599] ------------[cut here]------------ [4616.027779] WARNING: CPU: 4 PID: 99634 at block/blk-lib.c:50 __blkdev_issue_discard+0x16a/0x1a0 [4616.140663] RIP: 0010:__blkdev_issue_discard+0x16a/0x1a0 [4616.146601] Code: 24 4c 89 20 31 c0 e9 fe fe ff ff c1 e8 09 8d 48 ff 4c 89 f0 4c 09 e8 48 85 c1 0f 84 55 ff ff ff b8 ea ff ff ff e9 df fe ff ff <0f> 0b 48 8d 74 24 08 e8 ea d6 00 00 48 c7 c6 20 1e 89 ab 48 c7 c7 [4616.167567] RSP: 0018:ffffaab88cbffca8 EFLAGS: 00010246 [4616.173406] RAX: ffff9ba1f9e44678 RBX: 0000000000000000 RCX: ffff9ba1c9792080 [4616.181376] RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff9ba1c9792080 [4616.189345] RBP: 0000000000000cc0 R08: ffffaab88cbffd10 R09: 0000000000000000 [4616.197317] R10: 0000000000000012 R11: 0000000000000000 R12: 0000000000000000 [4616.205288] R13: 0000000000400000 R14: 0000000000000cc0 R15: ffff9ba1c9792080 [4616.213259] FS: 00007f9a5534e980(0000) GS:ffff9ba1b7c80000(0000) knlGS:0000000000000000 [4616.222298] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [4616.228719] CR2: 000055a390a4c518 CR3: 0000000123e40006 CR4: 0000000001706e0 [4616.236689] Call Trace: [4616.239428] blkdev_issue_discard+0x52/0xb0 [4616.244108] blkdev_common_ioctl+0x43c/0xa00 [4616.248883] blkdev_ioctl+0x116/0x280 [4616.252977] __x64_sys_ioctl+0x8a/0xc0 [4616.257163] do_syscall_64+0x5c/0x90 [4616.261164] ? handle_mm_fault+0xc5/0x2a0 [4616.265652] ? do_user_addr_fault+0x1d8/0x690 [4616.270527] ? do_syscall_64+0x69/0x90 [4616.274717] ? exc_page_fault+0x62/0x150 [4616.279097] entry_SYSCALL_64_after_hwframe+0x63/0xcd [4616.284748] RIP: 0033:0x7f9a55398c6b	N/A	More Details
CVE-2025-40317	In the Linux kernel, the following vulnerability has been resolved: regmap: slimbus: fix bus_context pointer in regmap init calls Commit 4e65bda8273c ("ASoC: wcd934x: fix error handling in wcd934x_codec_parse_data()") revealed the problem in the slimbus regmap. That commit breaks audio playback, for instance, on sdm845 Thundercomm Dragonboard 845c board: Unable to handle kernel paging request at virtual address ffff8000847cbad4 ... CPU: 5 UID: 0 PID: 776 Comm: aplay Not tainted 6.18.0-rc1-00028-g7ea30958b305 #11 PREEMPT Hardware name: Thundercomm Dragonboard 845c (DT) ... Call trace: slim_xfer_msg+0x24/0x1ac [slimbus] (P) slim_read+0x48/0x74 [slimbus] regmap_slimbus_read+0x18/0x24 [regmap_slimbus] _regmap_raw_read+0xe8/0x174 _regmap_bus_read+0x44/0x80 _regmap_read+0x60/0xd8 _regmap_update_bits+0xf4/0x140 _regmap_select_page+0xa8/0x124 _regmap_raw_write_impl+0x3b8/0x65c _regmap_bus_raw_write+0x60/0x80 _regmap_write+0x58/0xc0 regmap_write+0x4c/0x80 wcd934x_hw_params+0x494/0x8b8 [snd_soc_wcd934x] snd_soc_dai_hw_params+0x3c/0x7c [snd_soc_core] __soc_pcm_hw_params+0x22c/0x634 [snd_soc_core] dpcm_be_dai_hw_params+0x1d4/0x38c [snd_soc_core] dpcm_fe_dai_hw_params+0x9c/0x17c [snd_soc_core] snd_pcm_hw_params+0x124/0x464 [snd_pcm] snd_pcm_common_ioctl+0x110c/0x1820 [snd_pcm] snd_pcm_ioctl+0x34/0x4c [snd_pcm] __arm64_sys_ioctl+0xac/0x104 invoke_syscall+0x48/0x104 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xec el0t_64_sync_handler+0xa0/0xf0 el0t_64_sync+0x198/0x19c The __devm_regmap_init_slimbus() started to be used instead of __regmap_init_slimbus() after the commit mentioned above and turns out the incorrect bus_context pointer (3rd argument) was used in __devm_regmap_init_slimbus(). It should be just "slimbus" (which is equal to &slimbus->dev). Correct it. The wcd934x codec seems to be the only or the first user of devm_regmap_init_slimbus() but we should fix it till the point where __devm_regmap_init_slimbus() was introduced therefore two "Fixes" tags. While at this, also correct the same argument in __regmap_init_slimbus().	N/A	More Details
CVE-2025-40318	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: fix race in hci_cmd_sync_dequeue_once hci_cmd_sync_dequeue_once() does lookup and then cancel the entry under two separate lock sections. Meanwhile, hci_cmd_sync_work() can also delete the same entry, leading to double list_del() and "UAF". Fix this by holding cmd_sync_work_lock across both lookup and cancel, so that the entry cannot be removed concurrently.	N/A	More Details
CVE-2025-40319	In the Linux kernel, the following vulnerability has been resolved: bpf: Sync pending IRQ work before freeing ring buffer Fix a race where irq_work can be queued in bpf_ringbuf_commit() but the ring buffer is freed before the work executes. In the syzbot reproducer, a BPF program attached to sched_switch triggers bpf_ringbuf_commit(), queuing an irq_work. If the ring buffer is freed before this work executes, the irq_work thread may accesses freed memory. Calling `irq_work_sync(&rb->work)` ensures that all pending irq_work complete before freeing the buffer.	N/A	More Details

CVE-2025-40320	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential cfid UAF in smb2_query_info_compound When smb2_query_info_compound() retries, a previously allocated cfid may have been freed in the first attempt. Because cfid wasn't reset on replay, later cleanup could act on a stale pointer, leading to a potential use-after-free. Reinitialize cfid to NULL under the replay label. Example trace (trimmed): refcount_t: underflow; use-after-free. WARNING: CPU: 1 PID: 11224 at ../lib/refcount.c:28 refcount_warn_saturate+0x9c/0x110 [...] RIP: 0010:refcount_warn_saturate+0x9c/0x110 [...] Call Trace: <TASK> smb2_query_info_compound+0x29c/0x5c0 [cifs f90b72658819bd21c94769b6a652029a07a7172f] ? step_into+0x10d/0x690 ? __legitimize_path+0x28/0x60 smb2_queryfs+0x6a/0xf0 [cifs f90b72658819bd21c94769b6a652029a07a7172f] smb311_queryfs+0x12d/0x140 [cifs f90b72658819bd21c94769b6a652029a07a7172f] ? kmem_cache_alloc+0x18a/0x340 ? getname_flags+0x46/0x1e0 cifs_statfs+0x9f/0x2b0 [cifs f90b72658819bd21c94769b6a652029a07a7172f] statfs_by_dentry+0x67/0x90 vfs_statfs+0x16/0xd0 user_statfs+0x54/0xa0 __do_sys_statfs+0x20/0x50 do_syscall_64+0x58/0x80	N/A	More Details
CVE-2025-40321	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: fix crash while sending Action Frames in standalone AP Mode Currently, whenever there is a need to transmit an Action frame, the brcmfmac driver always uses the P2P vif to send the "actframe" IOVAR to firmware. The P2P interfaces were available when wpa_supplicant is managing the wlan interface. However, the P2P interfaces are not created/initialized when only hostapd is managing the wlan interface. And if hostapd receives an ANQP Query REQ Action frame even from an un-associated STA, the brcmfmac driver tries to use an uninitialized P2P vif pointer for sending the IOVAR to firmware. This NULL pointer dereferencing triggers a driver crash. [1417.074538] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [...] [1417.075188] Hardware name: Raspberry Pi 4 Model B Rev 1.5 (DT) [...] [1417.075653] Call trace: [1417.075662] brcmf_p2p_send_action_frame+0x23c/0xc58 [brcmfmac] [1417.075738] brcmf_cfg80211_mgmt_tx+0x304/0x5c0 [brcmfmac] [1417.075810] cfg80211_mlme_mgmt_tx+0x1b0/0x428 [cfg80211] [1417.076067] nl80211_tx_mgmt+0x238/0x388 [cfg80211] [1417.076281] genl_family_rcv_msg_doit+0xe0/0x158 [1417.076302] genl_rcv_msg+0x220/0x2a0 [1417.076317] netlink_rcv_skb+0x68/0x140 [1417.076330] genl_rcv+0x40/0x60 [1417.076343] netlink_unicast+0x330/0x3b8 [1417.076357] netlink_sendmsg+0x19c/0x3f8 [1417.076370] __sock_sendmsg+0x64/0xc0 [1417.076391] ____sys_sendmsg+0x268/0x2a0 [1417.076408] ___sys_sendmsg+0xb8/0x118 [1417.076427] __sys_sendmsg+0x90/0xf8 [1417.076445] __arm64_sys_sendmsg+0x2c/0x40 [1417.076465] invoke_syscall+0x50/0x120 [1417.076486] el0_svc_common.constprop.0+0x48/0xf0 [1417.076506] do_el0_svc+0x24/0x38 [1417.076525] el0_svc+0x30/0x100 [1417.076548] el0t_64_sync_handler+0x100/0x130 [1417.076569] el0t_64_sync+0x190/0x198 [1417.076589] Code: f9401e80 aa1603e2 f9403be1 5280e483 (f9400000) Fix this, by always using the vif corresponding to the wdev on which the Action frame Transmission request was initiated by the userspace. This way, even if P2P vif is not available, the IOVAR is sent to firmware on AP vif and the ANQP Query RESP Action frame is transmitted without crashing the driver. Move init_completion() for "send_af_done" from brcmf_p2p_create_p2pdev() to brcmf_p2p_attach(). Because the former function would not get executed when only hostapd is managing wlan interface, and it is not safe to do reinit_completion() later in brcmf_p2p_tx_action_frame(), without any prior init_completion(). And in the brcmf_p2p_tx_action_frame() function, the condition check for P2P Presence response frame is not needed, since the wpa_supplicant is properly sending the P2P Presense Response frame on the P2P-GO vif instead of the P2P-Device vif. [Cc stable]	N/A	More Details
CVE-2025-40322	In the Linux kernel, the following vulnerability has been resolved: fbdev: bitblit: bound-check glyph index in bit_putcs* bit_putcs_aligned()/unaligned() derived the glyph pointer from the character value masked by 0xff/0x1ff, which may exceed the actual font's glyph count and read past the end of the built-in font array. Clamp the index to the actual glyph count before computing the address. This fixes a global out-of-bounds read reported by syzbot.	N/A	More Details
CVE-2025-40323	In the Linux kernel, the following vulnerability has been resolved: fbcon: Set fb_display[i]->mode to NULL when the mode is released Recently, we discovered the following issue through syzkaller: BUG: KASAN: slab-use-after-free in fb_mode_is_equal+0x285/0x2f0 Read of size 4 at addr ff11000001b3c69c by task syz.xxx ... Call Trace: <TASK> dump_stack_lvl+0xab/0xe0 print_address_description.constprop.0+0x2c/0x390 print_report+0xb9/0x280 kasan_report+0xb8/0xf0 fb_mode_is_equal+0x285/0x2f0 fbcon_mode_deleted+0x129/0x180 fb_set_var+0xe7f/0x11d0 do_fb_ioctl+0x6a0/0x750 fb_ioctl+0xe0/0x140 __x64_sys_ioctl+0x193/0x210 do_syscall_64+0x5f/0x9c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e Based on experimentation and analysis, during framebuffer unregistration, only the memory of fb_info->modelist is freed, without setting the corresponding fb_display[i]->mode to NULL for the freed modes. This leads to UAF issues during subsequent accesses. Here's an example of reproduction steps: 1. With /dev/fb0 already registered in the system, load a kernel module to register a new device /dev/fb1; 2. Set fb1's mode to the global fb_display[] array (via FBIOPUT_CON2FBMAP); 3. Switch console from fb to VGA (to allow normal rmmod of the ko); 4. Unload the kernel module, at this point fb1's modelist is freed, leaving a wild pointer in fb_display[]; 5. Trigger the bug via system calls through fb0 attempting to delete a mode from fb0. Add a check in do_unregister_framebuffer(): if the mode to be freed exists in fb_display[], set the corresponding mode pointer to NULL.	N/A	More Details
CVE-2025-40324	In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix crash in nfsd4_read_release() When tracing is enabled, the trace_nfsd_read_done trace point crashes during the pynfs read.testNoFh test.	N/A	More Details
CVE-2025-40326	In the Linux kernel, the following vulnerability has been resolved: NFSD: Define actions for the new time_deleg FATTR4 attributes NFSv4 clients won't send legitimate GETATTR requests for these new attributes because they are intended to be used only with CB_GETATTR and SETATTR. But NFSD has to do something besides crashing if it ever sees a GETATTR request that queries these attributes. RFC 8881 Section 18.7.3 states: > The server MUST return a value for each attribute that the client > requests if the attribute is supported by the server for the > target file system. If the server does not support a particular > attribute on the target file system, then it MUST NOT return the > attribute value and MUST NOT set the attribute bit in the result > bitmap. The server MUST return an error if it supports an > attribute on the target but cannot obtain its value. In that case, > no attribute values will be returned. Further, RFC 9754 Section 5 states: > These new attributes are invalid to be used with GETATTR, VERIFY, > and NVERIFY, and they can only be used with CB_GETATTR and SETATTR > by a client holding an appropriate delegation. Thus there does not appear to be a specific server response mandated by specification. Taking the guidance that querying these attributes via GETATTR is "invalid", NFSD will return nfserr_inval, failing the request entirely.	N/A	More Details
CVE-2022-50614	In the Linux kernel, the following vulnerability has been resolved: misc: pci_endpoint_test: Fix pci_endpoint_test_{copy,write,read}() panic The dma_map_single() doesn't permit zero length mapping. It causes a follow panic. A panic was reported on arm64: [60.137988] ----------[cut here]---------- [60.142630] kernel BUG at kernel/dma/swiotlb.c:624! [60.147508] Internal error: Oops - BUG: 0 [#1] PREEMPT SMP [60.152992] Modules linked in: dw_hdmi_cec crct10dif_ce simple_bridge rcar_fdp1 vsp1 rcar_vin videobuf2_vmalloc rcar_csi2 v4l2_mem2mem videobuf2_dma_contig videobuf2_memops pci_endpoint_test videobuf2_v4l2 videobuf2_common rcar_fcp v4l2_fwnode v4l2_asyn c videodev mc gpio_bd9571mwv max9611 pwm_rcar ccree at24 authenc libdes phy_rcar_gen3_usb3 usb_dmac display_connector pwm_bl [60.186252] CPU: 0 PID: 508 Comm: pcitest Not tainted 6.0.0-rc1rpci-dev+ #237 [60.193387] Hardware name: Renesas Salvator-X 2nd version board based on r8a77951 (DT) [60.201302] pstate: 00000005 (nzcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [60.208263] pc : swiotlb_tbl_map_single+0x2c0/0x590 [60.213149] lr : swiotlb_map+0x88/0x1f0 [60.216982] sp : ffff80000a883bc0 [60.220292] x29: ffff80000a883bc0 x28: 0000000000000000 x27: 0000000000000000 [60.227430] x26: 0000000000000000 x25: ffff0004c0da20d0 x24: ffff80000a1f77c0 [60.234567] x23: 0000000000000002 x22: 0001000040000010 x21: 000000007a000000 [60.241703] x20: 0000000000200000 x19: 0000000000000000 x18: 0000000000000000 [60.248840] x17: 0000000000000000 x16: 0000000000000000 x15: ffff0006ff7b9180 [60.255977] x14: ffff0006ff7b9180 x13: 0000000000000000 x12: 0000000000000000 [60.263113] x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 [60.270249] x8 :	N/A	More Details

	0001000000000010 x7 : ffff0004c6754b20 x6 : 0000000000000000 [60.277385] x5 : ffff0004c0da2090 x4 : 0000000000000000 x3 : 0000000000000001 [60.284521] x2 : 0000000040000000 x1 : 0000000000000000 x0 : 0000000040000010 [60.291658] Call trace: [60.294100] swiotlb_tbl_map_single+0x2c0/0x590 [60.298629] swiotlb_map+0x88/0x1f0 [60.302115] dma_map_page_attrs+0x188/0x230 [60.306299] pci_endpoint_test_ioctl+0x5e4/0xd90 [pci_endpoint_test] [60.312660] __arm64_sys_ioctl+0xa8/0xf0 [60.316583] invoke_syscall+0x44/0x108 [60.320334] el0_svc_common.constprop.0+0xcc/0xf0 [60.325038] do_el0_svc+0x2c/0xb8 [60.328351] el0_svc+0x2c/0x88 [60.331406] el0t_64_sync_handler+0xb8/0xc0 [60.335587] el0t_64_sync+0x18c/0x190 [60.339251] Code: 52800013 d2e00414 35fff45c d503201f (d4210000) [60.345344] ---[end trace 0000000000000000]--- To fix it, this patch adds a checking the payload length if it is zero.		
CVE-2025-40315	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_fs: Fix epfile null pointer access after ep enable. A race condition occurs when ffs_func_eps_enable() runs concurrently with ffs_data_reset(). The ffs_data_clear() called in ffs_data_reset() sets ffs->epfiles to NULL before resetting ffs->eps_count to 0, leading to a NULL pointer dereference when accessing epfile->ep in ffs_func_eps_enable() after successful usb_ep_enable(). The ffs->epfiles pointer is set to NULL in both ffs_data_clear() and ffs_data_close() functions, and its modification is protected by the spinlock ffs->eps_lock. And the whole ffs_func_eps_enable() function is also protected by ffs->eps_lock. Thus, add NULL pointer handling for ffs->epfiles in the ffs_func_eps_enable() function to fix issues	N/A	More Details
CVE-2022-50615	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel/uncore: Fix reference count leak in snr_uncore_mmio_map() pci_get_device() will increase the reference count for the returned pci_dev, so snr_uncore_get_mc_dev() will return a pci_dev with its reference count increased. We need to call pci_dev_put() to decrease the reference count. Let's add the missing pci_dev_put().	N/A	More Details
CVE-2022-50616	In the Linux kernel, the following vulnerability has been resolved: regulator: core: Use different devices for resource allocation and DT lookup Following by the below discussion, there's the potential UAF issue between regulator and mfd. https://lore.kernel.org/all/20221128143601.1698148-1-yangyingliang@huawei.com/ From the analysis of Yingliang CPU A |CPU B mt6370_probe() | devm_mfd_add_devices() | |mt6370_regulator_probe() | regulator_register() | //allocate init_data and add it to devres | regulator_of_get_init_data() i2c_unregister_device() | device_del() | devres_release_all() | // init_data is freed | release_nodes() | | // using init_data causes UAF | regulator_register() It's common to use mfd core to create child device for the regulator. In order to do the DT lookup for init data, the child that registered the regulator would pass its parent as the parameter. And this causes init data resource allocated to its parent, not itself. The issue happen when parent device is going to release and regulator core is still doing some operation of init data constraint for the regulator of child device. To fix it, this patch expand 'regulator_register' API to use the different devices for init data allocation and DT lookup.	N/A	More Details
CVE-2022-50617	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/powerplay/psm: Fix memory leak in power state init Commit 902bc65de0b3 ("drm/amdgpu/powerplay/psm: return an error in power state init") made the power state init function return early in case of failure to get an entry from the powerplay table, but it missed to clean up the allocated memory for the current power state before returning.	N/A	More Details
CVE-2022-50618	In the Linux kernel, the following vulnerability has been resolved: mmc: meson-gx: fix return value check of mmc_add_host() mmc_add_host() may return error, if we ignore its return value, it will lead two issues: 1. The memory that allocated in mmc_alloc_host() is leaked. 2. In the remove() path, mmc_remove_host() will be called to delete device, but it's not added yet, it will lead a kernel crash because of null-ptr-deref in device_del(). Fix this by checking the return value and goto error path which will call mmc_free_host().	N/A	More Details
CVE-2022-50619	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix memory leak in kfd_mem_dmamap_userptr() If the number of pages from the userptr BO differs from the SG BO then the allocated memory for the SG table doesn't get freed before returning -EINVAL, which may lead to a memory leak in some error paths. Fix this by checking the number of pages before allocating memory for the SG table.	N/A	More Details
CVE-2022-50620	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to invalidate dcc->f2fs_issue_discard in error path Syzbot reports a NULL pointer dereference issue as below: __refcount_add include/linux/refcount.h:193 [inline] __refcount_inc include/linux/refcount.h:250 [inline] refcount_inc include/linux/refcount.h:267 [inline] get_task_struct include/linux/sched/task.h:110 [inline] kthread_stop+0x34/0x1c0 kernel/kthread.c:703 f2fs_stop_discard_thread+0x3c/0x5c fs/f2fs/segment.c:1638 kill_f2fs_super+0x5c/0x194 fs/f2fs/super.c:4522 deactivate_locked_super+0x70/0xe8 fs/super.c:332 deactivate_super+0xd0/0xd4 fs/super.c:363 cleanup_mnt+0x1f8/0x234 fs/namespace.c:1186 __cleanup_mnt+0x20/0x30 fs/namespace.c:1193 task_work_run+0xc4/0x14c kernel/task_work.c:177 exit_task_work include/linux/task_work.h:38 [inline] do_exit+0x26c/0xbe0 kernel/exit.c:795 do_group_exit+0x60/0xe8 kernel/exit.c:925 __do_sys_exit_group kernel/exit.c:936 [inline] __se_sys_exit_group kernel/exit.c:934 [inline] __wake_up_parent+0x0/0x40 kernel/exit.c:934 __invoke_syscall arch/arm64/kernel/syscall.c:38 [inline] invoke_syscall arch/arm64/kernel/syscall.c:52 [inline] el0_svc_common+0x138/0x220 arch/arm64/kernel/syscall.c:142 do_el0_svc+0x48/0x164 arch/arm64/kernel/syscall.c:206 el0_svc+0x58/0x150 arch/arm64/kernel/entry-common.c:636 el0t_64_sync_handler+0x84/0xf0 arch/arm64/kernel/entry-common.c:654 el0t_64_sync+0x18c/0x190 arch/arm64/kernel/entry.S:581 The root cause of this issue is in error path of f2fs_start_discard_thread(), it missed to invalidate dcc->f2fs_issue_discard, later kthread_stop() may access invalid pointer.	N/A	More Details
CVE-2022-50621	In the Linux kernel, the following vulnerability has been resolved: dm: verity-loadpin: Only trust verity targets with enforcement Verity targets can be configured to ignore corrupted data blocks. LoadPin must only trust verity targets that are configured to perform some kind of enforcement when data corruption is detected, like returning an error, restarting the system or triggering a panic.	N/A	More Details
CVE-2022-50622	In the Linux kernel, the following vulnerability has been resolved: ext4: fix potential memory leak in ext4_fc_record_modified_inode() As krealloc may return NULL, in this case 'state->fc_modified_inodes' may not be freed by krealloc, but 'state->fc_modified_inodes' already set NULL. Then will lead to 'state->fc_modified_inodes' memory leak.	N/A	More Details
CVE-2022-50623	In the Linux kernel, the following vulnerability has been resolved: fpga: prevent integer overflow in dfl_feature_ioctl_set_irq() The "hdr.count * sizeof(s32)" multiplication can overflow on 32 bit systems leading to memory corruption. Use array_size() to fix that.	N/A	More Details
CVE-2025-40316	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Fix device use-after-free on unbind A recent change fixed device reference leaks when looking up drm platform device driver data during bind() but failed to remove a partial fix which had been added by commit 80805b62ea5b ("drm/mediatek: Fix kobject put for component sub-drivers"). This results in a reference imbalance on component bind() failures and on unbind() which could lead to a user-after-free. Make sure to only drop the references after retrieving the driver data by effectively reverting the previous partial fix. Note that holding a reference to a device does not prevent its driver data from going away so there is no point in keeping the reference.	N/A	More Details
CVE-2025-40314	In the Linux kernel, the following vulnerability has been resolved: usb: cdns3: gadget: Use-after-free during failed initialization and exit of cdnsp gadget In the __cdnsp_gadget_init() and cdnsp_gadget_exit() functions, the gadget structure (pdev->gadget) was freed before its endpoints. The endpoints are linked via the ep_list in the gadget structure. Freeing the gadget first leaves dangling pointers in the endpoint list. When the endpoints are subsequently freed, this results in a use-after-free. Fix: By separating the usb_del_gadget_udc() operation into distinct "del" and "put" steps, cdnsp_gadget_free_endpoints() can be executed prior to the final release of the gadget structure with usb_put_gadget(). A patch similar to bb9c74a5bd14("usb: dwc3: gadget: Free gadget structure only after freeing	N/A	More Details

	endpoints").		
CVE-2025-40291	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix regbuf vector size truncation There is a report of io_estimate_bvec_size() truncating the calculated number of segments that leads to corruption issues. Check it doesn't overflow "int"s used later. Rough but simple, can be improved on top.	N/A	More Details
CVE-2025-40302	In the Linux kernel, the following vulnerability has been resolved: media: videobuf2: forbid remove_bufs when legacy fileio is active vb2_ioctl_remove_bufs() call manipulates queue internal buffer list, potentially overwriting some pointers used by the legacy fileio access mode. Forbid that ioctl when fileio is active to protect internal queue state between subsequent read/write calls.	N/A	More Details
CVE-2025-40292	In the Linux kernel, the following vulnerability has been resolved: virtio-net: fix received length check in big packets Since commit 4959aebba8c0 ("virtio-net: use mtu size as buffer length for big packets"), when guest gso is off, the allocated size for big packets is not MAX_SKB_FRAGS * PAGE_SIZE anymore but depends on negotiated MTU. The number of allocated frags for big packets is stored in vi->big_packets_num_skbfrags. Because the host announced buffer length can be malicious (e.g. the host vhost_net driver's get_rx_bufs is modified to announce incorrect length), we need a check in virtio_net receive path. Currently, the check is not adapted to the new change which can lead to NULL page pointer dereference in the below while loop when receiving length that is larger than the allocated one. This commit fixes the received length check corresponding to the new change.	N/A	More Details
CVE-2025-40293	In the Linux kernel, the following vulnerability has been resolved: iommufd: Don't overflow during division for dirty tracking If pgshift is 63 then BITS_PER_TYPE(*bitmap->bitmap) * pgsize will overflow to 0 and this triggers divide by 0. In this case the index should just be 0, so reorganize things to divide by shift and avoid hitting any overflows.	N/A	More Details
CVE-2025-40294	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix OOB access in parse_adv_monitor_pattern() In the parse_adv_monitor_pattern() function, the value of the 'length' variable is currently limited to HCI_MAX_EXT_AD_LENGTH(251). The size of the 'value' array in the mgmt_adv_pattern structure is 31. If the value of 'pattern[i].length' is set in the user space and exceeds 31, the 'patterns[i].value' array can be accessed out of bound when copied. Increasing the size of the 'value' array in the 'mgmt_adv_pattern' structure will break the userspace. Considering this, and to avoid OOB access revert the limits for 'offset' and 'length' back to the value of HCI_MAX_AD_LENGTH. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-40295	In the Linux kernel, the following vulnerability has been resolved: fscrypt: fix left shift underflow when inode->i_blkbits > PAGE_SHIFT When simulating an nvme device on qemu with both logical_block_size and physical_block_size set to 8 KiB, an error trace appears during partition table reading at boot time. The issue is caused by inode->i_blkbits being larger than PAGE_SHIFT, which leads to a left shift of -1 and triggering a UBSAN warning. [2.697306] ------------[cut here]------------ [2.697309] UBSAN: shift-out-of-bounds in fs/crypto/inline_crypt.c:336:37 [2.697311] shift exponent -1 is negative [2.697315] CPU: 3 UID: 0 PID: 274 Comm: (udev-worker) Not tainted 6.18.0-rc2+ #34 PREEMPT(voluntary) [2.697317] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [2.697320] Call Trace: [2.697324] <TASK> [2.697325] dump_stack_lvl+0x76/0xa0 [2.697340] dump_stack+0x10/0x20 [2.697342] __ubsan_handle_shift_out_of_bounds+0x1e3/0x390 [2.697351] bh_get_inode_and_lblk_num.cold+0x12/0x94 [2.697359] fscrypt_set_bio_crypt_ctx_bh+0x44/0x90 [2.697365] submit_bh_wbc+0xb6/0x190 [2.697370] block_read_full_folio+0x194/0x270 [2.697371] ? __pfx_blkdev_get_block+0x10/0x10 [2.697375] ? __pfx_blkdev_read_folio+0x10/0x10 [2.697377] blkdev_read_folio+0x18/0x30 [2.697379] filemap_read_folio+0x40/0xe0 [2.697382] filemap_get_pages+0x5ef/0x7a0 [2.697385] ? mmap_region+0x63/0xd0 [2.697389] filemap_read+0x11d/0x520 [2.697392] blkdev_read_iter+0x7c/0x180 [2.697393] vfs_read+0x261/0x390 [2.697397] ksys_read+0x71/0xf0 [2.697398] __x64_sys_read+0x19/0x30 [2.697399] x64_sys_call+0x1e88/0x26a0 [2.697405] do_syscall_64+0x80/0x670 [2.697410] ? __x64_sys_newfstat+0x15/0x20 [2.697414] ? x64_sys_call+0x204a/0x26a0 [2.697415] ? do_syscall_64+0xb8/0x670 [2.697417] ? irqentry_exit_to_user_mode+0x2e/0x2a0 [2.697420] ? irqentry_exit+0x43/0x50 [2.697421] ? exc_page_fault+0x90/0x1b0 [2.697422] entry_SYSCALL_64_after_hwframe+0x76/0x7e [2.697425] RIP: 0033:0x75054cba4a06 [2.697426] Code: 5d e8 41 8b 93 08 03 00 00 59 5e 48 83 f8 fc 75 19 83 e2 39 83 fa 08 75 11 e8 26 ff ff ff 66 0f 1f 44 00 00 48 8b 45 10 0f 05 <48> 8b 5d f8 c9 c3 0f 1f 40 00 f3 0f 1e fa 55 48 89 e5 48 83 ec 08 [2.697427] RSP: 002b:00007fff973723a0 EFLAGS: 00000202 ORIG_RAX: 0000000000000000 [2.697430] RAX: ffffffffffffffda RBX: 00005ea9a2c02760 RCX: 000075054cba4a06 [2.697432] RDX: 0000000000002000 RSI: 000075054c190000 RDI: 000000000000001b [2.697433] RBP: 00007fff973723c0 R08: 0000000000000000 R09: 0000000000000000 [2.697434] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [2.697434] R13: 00005ea9a2c027c0 R14: 00005ea9a2be5608 R15: 00005ea9a2be55f0 [2.697436] </TASK> [2.697436] ---[end trace]--- This situation can happen for block devices because when CONFIG_TRANSPARENT_HUGEPAGE is enabled, the maximum logical_block_size is 64 KiB. set_init_blocksize() then sets the block device inode->i_blkbits to 13, which is within this limit. File I/O does not trigger this problem because for filesystems that do not support the FS_LBS feature, sb_set_blocksize() prevents sb->s_blocksize_bits from being larger than PAGE_SHIFT. During inode allocation, alloc_inode()->inode_init_always() assigns inode->i_blkbits from sb->s_blocksize_bits. Currently, only xfs_fs_type has the FS_LBS flag, and since xfs I/O paths do not reach submit_bh_wbc(), it does not hit the left-shift underflow issue. [EB: use folio_pos() and consolidate the two shifts by i_blkbits]	N/A	More Details
CVE-2025-40296	In the Linux kernel, the following vulnerability has been resolved: platform/x86: int3472: Fix double free of GPIO device during unregister regulator_unregister() already frees the associated GPIO device. On ThinkPad X9 (Lunar Lake), this causes a double free issue that leads to random failures when other drivers (typically Intel THC) attempt to allocate interrupts. The root cause is that the reference count of the pinctrl_intel_platform module unexpectedly drops to zero when this driver defers its probe. This behavior can also be reproduced by unloading the module directly. Fix the issue by removing the redundant release of the GPIO device during regulator unregistration.	N/A	More Details
CVE-2025-40297	In the Linux kernel, the following vulnerability has been resolved: net: bridge: fix use-after-free due to MST port state bypass syzbot reported[1] a use-after-free when deleting an expired fdb. It is due to a race condition between learning still happening and a port being deleted, after all its fdbs have been flushed. The port's state has been toggled to disabled so no learning should happen at that time, but if we have MST enabled, it will bypass the port's state, that together with VLAN filtering disabled can lead to fdb learning at a time when it shouldn't happen while the port is being deleted. VLAN filtering must be disabled because we flush the port VLANs when it's being deleted which will stop learning. This fix adds a check for the port's vlan group which is initialized to NULL when the port is getting deleted, that avoids the port state bypass. When MST is enabled there would be a minimal new overhead in the fast-path because the port's vlan group pointer is cache-hot. [1] https://syzkaller.appspot.com/bug?extid=dd280197f0f7ab3917be	N/A	More Details
CVE-2025-40298	In the Linux kernel, the following vulnerability has been resolved: gve: Implement settime64 with -EOPNOTSUPP ptp_clock_settime() assumes every ptp_clock has implemented settime64(). Stub it with -EOPNOTSUPP to prevent a NULL dereference.	N/A	More Details
CVE-2025-40299	In the Linux kernel, the following vulnerability has been resolved: gve: Implement gettimex64 with -EOPNOTSUPP gve implemented a ptp_clock for sole use of do_aux_work at this time. ptp_clock_gettime() and ptp_sys_offset() assume every ptp_clock has implemented either gettimex64 or gettime64. Stub gettimex64 and return -EOPNOTSUPP to prevent NULL dereferencing.	N/A	More Details
CVE-2025-40301	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: validate skb length for unknown CC opcode In hci_cmd_complete_evt(), if the command complete event has an unknown opcode, we assume the first byte of the remaining skb->data contains the return status. However, parameter data has previously been pulled in hci_event_func(), which may leave the skb empty. If so, using skb->data[0] for the return status uses un-init memory. The fix is to check skb->len before using skb->data.	N/A	More Details

CVE-2025-40303	In the Linux kernel, the following vulnerability has been resolved: btrfs: ensure no dirty metadata is written back for an fs with errors [BUG] During development of a minor feature (make sure all btrfs_bio::end_io() is called in task context), I noticed a crash in generic/388, where metadata writes triggered new works after btrfs_stop_all_workers(). It turns out that it can even happen without any code modification, just using RAID5 for metadata and the same workload from generic/388 is going to trigger the use-after-free. [CAUSE] If btrfs hits an error, the fs is marked as error, no new transaction is allowed thus metadata is in a frozen state. But there are some metadata modifications before that error, and they are still in the btree inode page cache. Since there will be no real transaction commit, all those dirty folios are just kept as is in the page cache, and they can not be invalidated by invalidate_inode_pages2() call inside close_ctree(), because they are dirty. And finally after btrfs_stop_all_workers(), we call iput() on btree inode, which triggers writeback of those dirty metadata. And if the fs is using RAID56 metadata, this will trigger RMW and queue new works into rmw_workers, which is already stopped, causing warning from queue_work() and use-after-free. [FIX] Add a special handling for write_one_eb(), that if the fs is already in an error state, immediately mark the bbio as failure, instead of really submitting them. Then during close_ctree(), iput() will just discard all those dirty tree blocks without really writing them back, thus no more new jobs for already stopped-and-freed workqueues. The extra discard in write_one_eb() also acts as an extra safenet. E.g. the transaction abort is triggered by some extent/free space tree corruptions, and since extent/free space tree is already corrupted some tree blocks may be allocated where they shouldn't be (overwriting existing tree blocks). In that case writing them back will further corrupting the fs.	N/A	More Details
CVE-2025-40313	In the Linux kernel, the following vulnerability has been resolved: ntfs3: pretend $Extend records as regular files Since commit af153bb63a33 ("vfs: catch invalid modes in may_open()") requires any inode be one of S_IFDIR/S_IFLNK/S_IFREG/S_IFCHR/S_IFBLK/ S_IFIFO/S_IFSOCK type, use S_IFREG for $Extend records.	N/A	More Details
CVE-2025-40304	In the Linux kernel, the following vulnerability has been resolved: fbdev: Add bounds checking in bit_putcs to fix vmalloc-out-of-bounds Add bounds checking to prevent writes past framebuffer boundaries when rendering text near screen edges. Return early if the Y position is off-screen and clip image height to screen boundary. Break from the rendering loop if the X position is off-screen. When clipping image width to fit the screen, update the character count to match the clipped width to prevent buffer size mismatches. Without the character count update, bit_putcs_aligned and bit_putcs_unaligned receive mismatched parameters where the buffer is allocated for the clipped width but cnt reflects the original larger count, causing out-of-bounds writes.	N/A	More Details
CVE-2025-40305	In the Linux kernel, the following vulnerability has been resolved: 9p/trans_fd: p9_fd_request: kick rx thread if EPOLLIN p9_read_work() doesn't set Rworksched and doesn't do schedule_work(m->rq) if list_empty(&m->req_list). However, if the pipe is full, we need to read more data and this used to work prior to commit aaec5a95d59615 ("pipe_read: don't wake up the writer if the pipe is still full"). p9_read_work() does p9_fd_read() -> ... -> anon_pipe_read() which (before the commit above) triggered the unnecessary wakeup. This wakeup calls p9_pollwake() which kicks p9_poll_workfn() -> p9_poll_mux(), p9_poll_mux() will notice EPOLLIN and schedule_work(&m->rq). This no longer happens after the optimization above, change p9_fd_request() to use p9_poll_mux() instead of only checking for EPOLLOUT.	N/A	More Details
CVE-2025-40306	In the Linux kernel, the following vulnerability has been resolved: orangefs: fix xattr related buffer overflow... Willy Tarreau <w@1wt.eu> forwarded me a message from Disclosure <disclosure@aisle.com> with the following warning: > The helper `xattr_key()` uses the pointer variable in the loop condition > rather than dereferencing it. As `key` is incremented, it remains non-NULL > (until it runs into unmapped memory), so the loop does not terminate on > valid C strings and will walk memory indefinitely, consuming CPU or hanging > the thread. I easily reproduced this with setfattr and getfattr, causing a kernel oops, hung user processes and corrupted orangefs files. Disclosure sent along a diff (not a patch) with a suggested fix, which I based this patch on. After xattr_key started working right, xfstest generic/069 exposed an xattr related memory leak that lead to OOM. xattr_key returns a hashed key. When adding xattrs to the orangefs xattr cache, orangefs used hash_add, a kernel hashing macro. hash_add also hashes the key using hash_log which resulted in additions to the xattr cache going to the wrong hash bucket. generic/069 tortures a single file and orangefs does a getattr for the xattr "security.capability" every time. Orangefs negative caches on xattrs which includes a kmalloc. Since adds to the xattr cache were going to the wrong bucket, every getattr for "security.capability" resulted in another kmalloc, none of which were ever freed. I changed the two uses of hash_add to hlist_add_head instead and the memory leak ceased and generic/069 quit throwing furniture.	N/A	More Details
CVE-2025-40307	In the Linux kernel, the following vulnerability has been resolved: exfat: validate cluster allocation bits of the allocation bitmap syzbot created an exfat image with cluster bits not set for the allocation bitmap. exfat-fs reads and uses the allocation bitmap without checking this. The problem is that if the start cluster of the allocation bitmap is 6, cluster 6 can be allocated when creating a directory with mkdir. exfat zeros out this cluster in exfat_mkdir, which can delete existing entries. This can reallocate the allocated entries. In addition, the allocation bitmap is also zeroed out, so cluster 6 can be reallocated. This patch adds exfat_test_bitmap_range to validate that clusters used for the allocation bitmap are correctly marked as in-use.	N/A	More Details
CVE-2025-40308	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: bcsp: receive data only if registered Currently, bcsp_recv() can be called even when the BCSP protocol has not been registered. This leads to a NULL pointer dereference, as shown in the following stack trace: KASAN: null-ptr-deref in range [0x0000000000000108-0x000000000000010f] RIP: 0010:bcsp_recv+0x13d/0x1740 drivers/bluetooth/hci_bcsp.c:590 Call Trace: <TASK> hci_uart_tty_receive+0x194/0x220 drivers/bluetooth/hci_ldisc.c:627 tiocsti+0x23c/0x2c0 drivers/tty/tty_io.c:2290 tty_ioctl+0x626/0xde0 drivers/tty/tty_io.c:2706 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:893 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 To prevent this, ensure that the HCI_UART_REGISTERED flag is set before processing received data. If the protocol is not registered, return -EUNATCH.	N/A	More Details
CVE-2025-40309	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SCO: Fix UAF on sco_conn_free BUG: KASAN: slab-use-after-free in sco_conn_free net/bluetooth/sco.c:87 [inline] BUG: KASAN: slab-use-after-free in kref_put include/linux/kref.h:65 [inline] BUG: KASAN: slab-use-after-free in sco_conn_put+0xdd/0x410 net/bluetooth/sco.c:107 Write of size 8 at addr ffff88811cb96b50 by task kworker/u17:4/352 CPU: 1 UID: 0 PID: 352 Comm: kworker/u17:4 Not tainted 6.17.0-rc5-g717368f83676 #4 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: hci13 hci_cmd_sync_work Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x10b/0x170 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x191/0x550 mm/kasan/report.c:482 kasan_report+0xc4/0x100 mm/kasan/report.c:595 sco_conn_free net/bluetooth/sco.c:87 [inline] kref_put include/linux/kref.h:65 [inline] sco_conn_put+0xdd/0x410 net/bluetooth/sco.c:107 sco_connect_cfm+0xb4/0xae0 net/bluetooth/sco.c:1441 hci_connect_cfm include/net/bluetooth/hci_core.h:2082 [inline] hci_conn_failed+0x20a/0x2e0 net/bluetooth/hci_conn.c:1313 hci_conn_unlink+0x55f/0x810 net/bluetooth/hci_conn.c:1121 hci_conn_del+0xb6/0x1110 net/bluetooth/hci_conn.c:1147 hci_abort_conn_sync+0x8c5/0xbb0 net/bluetooth/hci_sync.c:5689 hci_cmd_sync_work+0x281/0x380 net/bluetooth/hci_sync.c:332 process_one_work kernel/workqueue.c:3236 [inline] process_scheduled_works+0x77e/0x1040 kernel/workqueue.c:3319 worker_thread+0xbee/0x1200 kernel/workqueue.c:3400 kthread+0x3c7/0x870 kernel/kthread.c:463 ret_from_fork+0x13a/0x1e0 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> Allocated by task 31370: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x70 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:388 [inline] __kasan_kmalloc+0x82/0x90 mm/kasan/common.c:405 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4382 [inline] __kmalloc_noprof+0x22f/0x390 mm/slub.c:4394 kmalloc_noprof include/linux/slab.h:909 [inline] sk_prot_alloc+0xae/0x220 net/core/sock.c:2239 sk_alloc+0x34/0x5a0 net/core/sock.c:2295 bt_sock_alloc+0x3c/0x330 net/bluetooth/af_bluetooth.c:151 sco_sock_alloc net/bluetooth/sco.c:562 [inline] sco_sock_create+0xc0/0x350 net/bluetooth/sco.c:593 bt_sock_create+0x161/0x3b0 net/bluetooth/af_bluetooth.c:135 __sock_create+0x3ad/0x780 net/socket.c:1589 sock_create net/socket.c:1647 [inline] __sys_socket_create net/socket.c:1684 [inline] __sys_socket+0xd5/0x330 net/socket.c:1731 __do_sys_socket	N/A	More Details

	net/socket.c:1745 [inline] __se_sys_socket net/socket.c:1743 [inline] __x64_sys_socket+0x7a/0x90 net/socket.c:1743 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xc7/0x240 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 31374: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x70 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:576 poison_slab_object mm/kasan/common.c:243 [inline] __kasan_slab_free+0x3d/0x50 mm/kasan/common.c:275 kasan_slab_free include/linux/kasan.h:233 [inline] slab_free_hook mm/slub.c:2428 [inline] slab_free mm/slub.c:4701 [inline] kfree+0x199/0x3b0 mm/slub.c:4900 sk_prot_free net/core/sock.c:2278 [inline] __sk_destruct+0x4aa/0x630 net/core/sock.c:2373 sco_sock_release+0x2ad/0x300 net/bluetooth/sco.c:1333 __sock_release net/socket.c:649 [inline] sock_close+0xb8/0x230 net/socket.c:1439 __fput+0x3d1/0x9e0 fs/file_table.c:468 task_work_run+0x206/0x2a0 kernel/task_work.c:227 get_signal+0x1201/0x1410 kernel/signal.c:2807 arch_do_signal_or_restart+0x34/0x740 arch/x86/kernel/signal.c:337 exit_to_user_mode_loop+0x68/0xc0 kernel/entry/common.c:40 exit_to_user_mode_prepare include/linux/irq-entry-common.h:225 [inline] s ---truncated---		
CVE-2025-40310	In the Linux kernel, the following vulnerability has been resolved: amd/amdkfd: resolve a race in amdgpu_amdkfd_device_fini_sw There is race in amdgpu_amdkfd_device_fini_sw and interrupt. if amdgpu_amdkfd_device_fini_sw run in b/w kfd_cleanup_nodes and kfree(kfd), and KGD interrupt generated. kernel panic log: BUG: kernel NULL pointer dereference, address: 0000000000000098 amdgpu 0000:c8:00.0: amdgpu: Requesting 4 partitions through PSP PGD d78c68067 P4D d78c68067 kfd kfd: amdgpu: Allocated 3969056 bytes on gart PUD 1465b8067 PMD @ Oops: @002 [#1] SMP NOPTI kfd kfd: amdgpu: Total number of KFD nodes to be created: 4 CPU: 115 PID: @ Comm: swapper/115 Kdump: loaded Tainted: G S W OE K RIP: 0010:_raw_spin_lock_irqsave+0x12/0x40 Code: 89 e@ 41 5c c3 cc cc cc cc 66 66 2e Of 1f 84 00 00 00 00 00 OF 1f 40 00 Of 1f 44% 00 00 41 54 9c 41 5c fa 31 cO ba 01 00 00 00 <fO> OF b1 17 75 Ba 4c 89 e@ 41 Sc 89 c6 e8 07 38 5d RSP: 0018: ffffc90@1a6b0e28 EFLAGS: 00010046 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000018 0000000000000001 RSI: ffff8883bb623e00 RDI: 0000000000000098 ffff8883bb000000 RO8: ffff888100055020 ROO: ffff888100055020 0000000000000000 R11: 0000000000000000 R12: 0900000000000002 ffff888F2b97da0@ R14: @000000000000098 R15: ffff8883babdfo00 CS: 010 DS: 0000 ES: 0000 CRO: 0000000080050033 CR2: 0000000000000098 CR3: 0000000e7cae2006 CR4: 0000000002770ce0 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 0000000000000000 DR6: 00000000fffeO7FO DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> kgd2kfd_interrupt+@x6b/0x1f@ [amdgpu] ? amdgpu_fence_process+0xa4/0x150 [amdgpu] kfd kfd: amdgpu: Node: 0, interrupt_bitmap: 3 YcpxFl Rant tErace amdgpu_irq_dispatch+0x165/0x210 [amdgpu] amdgpu_ih_process+0x80/0x100 [amdgpu] amdgpu: Virtual CRAT table created for GPU amdgpu_irq_handler+0x1f/@x60 [amdgpu] __handle_irq_event_percpu+0x3d/0x170 amdgpu: Topology: Add dGPU node [0x74a2:0x1002] handle_irq_event+0x5a/@xcO handle_edge_irq+0x93/0x240 kfd kfd: amdgpu: KFD node 1 partition @ size 49148M asm_call_irq_on_stack+0xf/@x20 </IRQ> common_interrupt+0xb3/0x130 asm_common_interrupt+0x1le/0x40 5.10.134-010.a1i5000.a18.x86_64 #1	N/A	More Details
CVE-2025-40311	In the Linux kernel, the following vulnerability has been resolved: accel/habanalabs: support mapping cb with vmalloc-backed coherent memory When IOMMU is enabled, dma_alloc_coherent() with GFP_USER may return addresses from the vmalloc range. If such an address is mapped without VM_MIXEDMAP, vm_insert_page() will trigger a BUG_ON due to the VM_PFNMAP restriction. Fix this by checking for vmalloc addresses and setting VM_MIXEDMAP in the VMA before mapping. This ensures safe mapping and avoids kernel crashes. The memory is still driver-allocated and cannot be accessed directly by userspace.	N/A	More Details
CVE-2025-40312	In the Linux kernel, the following vulnerability has been resolved: jfs: Verify inode mode when loading from disk The inode mode loaded from corrupted disk can be invalid. Do like what commit 0a9e74051313 ("isofs: Verify inode mode when loading from disk") does.	N/A	More Details
CVE-2023-53777	In the Linux kernel, the following vulnerability has been resolved: erofs: kill hooked chains to avoid loops on deduplicated compressed images After heavily stressing EROFS with several images which include a hand-crafted image of repeated patterns for more than 46 days, I found two chains could be linked with each other almost simultaneously and form a loop so that the entire loop won't be submitted. As a consequence, the corresponding file pages will remain locked forever. It can be _only_ observed on data-deduplicated compressed images. For example, consider two chains with five pclusters in total: Chain 1: 2->3->4->5 -- The tail pcluster is 5; Chain 2: 5->1->2 -- The tail pcluster is 2. Chain 2 could link to Chain 1 with pcluster 5; and Chain 1 could link to Chain 2 at the same time with pcluster 2. Since hooked chains are all linked locklessly now, I have no idea how to simply avoid the race. Instead, let's avoid hooked chains completely until I could work out a proper way to fix this and end users finally tell us that it's needed to add it back. Actually, this optimization can be found with multi-threaded workloads (especially even more often on deduplicated compressed images), yet I'm not sure about the overall system impacts of not having this compared with implementation complexity.	N/A	More Details
CVE-2023-53779	In the Linux kernel, the following vulnerability has been resolved: mfd: dln2: Fix memory leak in dln2_probe() When dln2_setup_rx_urbs() in dln2_probe() fails, error out_free forgets to call usb_put_dev() to decrease the refcount of dln2->usb_dev. Fix this by adding usb_put_dev() in the error handling code of dln2_probe().	N/A	More Details
CVE-2025-62082	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nasir Uddin Generic Elements generic-elements-for-elementor allows Stored XSS.This issue affects Generic Elements: from n/a through <= 1.2.8.	N/A	More Details
CVE-2023-53851	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dp: Drop aux devices together with DP controller Using devres to depopulate the aux bus made sure that upon a probe deferral the EDP panel device would be destroyed and recreated upon next attempt. But the struct device which the devres is tied to is the DPUs (drm_dev->dev), which may be happen after the DP controller is torn down. Indications of this can be seen in the commonly seen EDID-hexdump full of zeros in the log, or the occasional/rare KASAN fault where the panel's attempt to read the EDID information causes a use after free on DP resources. It's tempting to move the devres to the DP controller's struct device, but the resources used by the device(s) on the aux bus are explicitly torn down in the error path. The KASAN-reported use-after-free also remains, as the DP aux "module" explicitly frees its devres-allocated memory in this code path. As such, explicitly depopulate the aux bus in the error path, and in the component unbind path, to avoid these issues. Patchwork: https://patchwork.freedesktop.org/patch/542163/	N/A	More Details
CVE-2025-12807	A security issue was discovered in DataMosaix Private Cloud, allowing users with low privilege to perform sensitive database operations through exposed API endpoints.	N/A	More Details
CVE-2025-13031	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.8.13 does not sanitize and escape some of its settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks	N/A	More Details
CVE-2025-13070	The CSV to SortTable WordPress plugin through 4.2 does not validate some shortcode attributes before using them to generate paths passed to include function/s, allowing any authenticated users such as contributor to perform LFI attacks.	N/A	More Details
CVE-2025-13071	The Custom Admin Menu WordPress plugin through 1.0.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	N/A	More Details

CVE-2025-13428	A vulnerability exists in the SecOps SOAR server. The custom integrations feature allowed an authenticated user with an "IDE role" to achieve Remote Code Execution (RCE) in the server. The flaw stemmed from weak validation of uploaded Python package code. An attacker could upload a package containing a malicious setup.py file, which would execute on the server during the installation process, leading to potential server compromise. No customer action is required. All customers have been automatically upgraded to the fixed version: 6.3.64 or higher.	N/A	More Details
CVE-2025-11838	A memory corruption vulnerability in WatchGuard Fireware OS may allow an unauthenticated attacker to trigger a Denial of Service (DoS) condition in 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 12.0 up to and including 12.11.4 and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-10285	The web interface of the Silicon Labs Simplicity Device Manager is exposed publicly and can be used to extract the NTLMv2 hash which an attacker could use to crack the user's domain password.	N/A	More Details
CVE-2025-66576	Remote Keyboard Desktop 1.0.1 enables remote attackers to execute system commands via the rundll32.exe exported function export, allowing unauthenticated code execution.	N/A	More Details
CVE-2025-66575	VeeVPN 1.6.1 contains an unquoted service path vulnerability in the VeePNService that allows remote attackers to execute code during startup or reboot with escalated privileges. Attackers can exploit this by providing a malicious service name, allowing them to inject commands and run as LocalSystem.	N/A	More Details
CVE-2025-14306	A directory traversal vulnerability exists in the CacheCleaner component of Robocode version 1.9.3.6. The recursivelyDelete method fails to properly sanitize file paths, allowing attackers to traverse directories and delete arbitrary files on the system. This vulnerability can be exploited by submitting specially crafted inputs that manipulate the file path, leading to potential unauthorized file deletions. https://robo-code.blogspot.com/	N/A	More Details
CVE-2025-14307	An insecure temporary file creation vulnerability exists in the AutoExtract component of Robocode version 1.9.3.6. The createTempFile method fails to securely create temporary files, allowing attackers to exploit race conditions and potentially execute arbitrary code or overwrite critical files. This vulnerability can be exploited by manipulating the temporary file creation process, leading to potential unauthorized actions.	N/A	More Details
CVE-2025-14308	An integer overflow vulnerability exists in the write method of the Buffer class in Robocode version 1.9.3.6. The method fails to properly validate the length of data being written, allowing attackers to cause an overflow, potentially leading to buffer overflows and arbitrary code execution. This vulnerability can be exploited by submitting specially crafted inputs that manipulate the data length, leading to potential unauthorized code execution.	N/A	More Details
CVE-2025-66574	TranzAxis 3.2.41.10.26 allows authenticated users to inject cross-site scripting via the `Open Object in Tree` endpoint, allowing attackers to steal session cookies and potentially escalate privileges.	N/A	More Details
CVE-2025-14310	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in rethinkdb.This issue affects rethinkdb: before 2.4.4.	N/A	More Details
CVE-2025-14311	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in JMRI.This issue affects JMRI: before 5.13.3.	N/A	More Details
CVE-2025-14321	Use-after-free in the WebRTC: Signaling component. This vulnerability affects Firefox < 146 and Firefox ESR < 140.6.	N/A	More Details
CVE-2025-66573	Solstice Pod API (version 5.5, 6.2) contains an unauthenticated API endpoint (`/api/config`) that exposes sensitive information such as the session key, server version, product details, and display name. Unauthorized users can extract live session information by accessing this endpoint without authentication.	N/A	More Details
CVE-2025-66572	Loaded Commerce 6.6 contains a client-side template injection vulnerability that allows unauthenticated attackers to execute code on the server via the search parameter.	N/A	More Details
CVE-2025-14324	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 146, Firefox ESR < 115.31, and Firefox ESR < 140.6.	N/A	More Details
CVE-2025-66571	UNA CMS versions 9.0.0-RC1 - 14.0.0-RC4 contain a PHP object injection vulnerability in BxBaseMenuSetAclLevel.php where the profile_id POST parameter is passed to PHP unserialize() without proper handling, allowing remote, unauthenticated attackers to inject arbitrary PHP objects and potentially write and execute arbitrary PHP code.	N/A	More Details
CVE-2025-14326	Use-after-free in the Audio/Video: GMP component. This vulnerability affects Firefox < 146.	N/A	More Details
CVE-2025-12026	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS's certificate request command could allow an authenticated privileged user to execute arbitrary code via specially crafted CLI commands.This vulnerability affects Fireware OS 12.0 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-12381	Improper Privilege Management vulnerability in AlgoSec Firewall Analyzer on Linux, 64 bit allows Privilege Escalation, Parameter Injection. A local user with access to the command line may escalate their privileges by abusing the parameters of a command that is approved in the sudoers file. This issue affects Firewall Analyzer: A33.0, A33.10.	N/A	More Details
CVE-2025-66562	TUUI is a desktop MCP client designed as a tool unitary utility integration. Prior to 1.3.4, a critical Remote Code Execution (RCE) vulnerability exists in Tuui due to an unsafe Cross-Site Scripting (XSS) flaw in the Markdown rendering component. Tuui allows the execution of arbitrary JavaScript within ECharts code blocks. Combined with an exposed IPC interface that allows spawning processes, an attacker can execute arbitrary system commands on the victim's machine simply by having them view a malicious Markdown message. This vulnerability is fixed in 1.3.4.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: hfs: fix missing hfs_bnode_get() in __hfs_bnode_create Syzbot found a		

CVE-2023-53862	kernel BUG in hfs_bnode_put(): kernel BUG at fs/hfs/bnode.c:466! invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 0 PID: 3634 Comm: kworker/u4:5 Not tainted 6.1.0-rc7-syzkaller-00190-g97ee9d1c1696 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022 Workqueue: writeback wb_workfn (flush-7:0) RIP: 0010:hfs_bnode_put+0x46f/0x480 fs/hfs/bnode.c:466 Code: 8a 80 ff e9 73 fe ff ff 89 d9 80 e1 07 80 c1 03 38 c1 0f 8c a0 fe ff ff 48 89 df e8 db 8a 80 ff e9 93 fe ff ff e8 a1 68 2c ff <0f> 0b e8 9a 68 2c ff 0f 0b 0f 1f 84 00 00 00 00 00 55 41 57 41 56 RSP: 0018:ffffc90003b4f258 EFLAGS: 00010293 RAX: ffffffff825e318f RBX: 0000000000000000 RCX: ffff8880739dd7c0 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc90003b4f430 R08: ffffffff825e2d9b R09: ffffed10045157d1 R10: ffffed10045157d1 R11: 1ffff110045157d0 R12: ffff8880228abe80 R13: ffff88807016c000 R14: dfffffc0000000000 R15: ffff8880228abe00 FS: 0000000000000000(0000) GS:ffff8880b9800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fa6ebe88718 CR3: 000000001e93d000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> hfs_write_inode+0x1bc/0xb40 write_inode fs/fs-writeback.c:1440 [inline] __writeback_single_inode+0x4d6/0x670 fs/fs-writeback.c:1652 writeback_sb_inodes+0xb3b/0x18f0 fs/fs-writeback.c:1878 __writeback_inodes_wb+0x125/0x420 fs/fs-writeback.c:1949 wb_writeback+0x440/0x7b0 fs/fs-writeback.c:2054 wb_check_start_all fs/fs-writeback.c:2176 [inline] wb_do_writeback fs/fs-writeback.c:2202 [inline] wb_workfn+0x827/0xef0 fs/fs-writeback.c:2235 process_one_work+0x877/0xdb0 kernel/workqueue.c:2289 worker_thread+0xb14/0x1330 kernel/workqueue.c:2436 kthread+0x266/0x300 kernel/kthread.c:376 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:306 </TASK> The BUG_ON() is triggered at here: /* Dispose of resources used by a node */ void hfs_bnode_put(struct hfs_bnode *node) { if (node) { <skipped> BUG_ON(!atomic_read(&node->refcnt)); <- we have issue here!!!! <skipped> } } By tracing the refcnt, I found the node is created by hfs_bmap_alloc() with refcnt 1. Then the node is used by hfs_btree_write(). There is a missing of hfs_bnode_get() after find the node. The issue happened in following path: <alloc> hfs_bmap_alloc hfs_bnode_find __hfs_bnode_create <- allocate a new node with refcnt 1. hfs_bnode_put <- decrease the refcnt <write> hfs_btree_write hfs_bnode_find __hfs_bnode_create hfs_bnode_findhash <- find the node without refcnt increased. hfs_bnode_put <- trigger the BUG_ON() since refcnt is 0.	N/A	More Details
CVE-2023-53853	In the Linux kernel, the following vulnerability has been resolved: netlink: annotate accesses to nlk->cb_running Both netlink_recvmsg() and netlink_native_seq_show() read nlk->cb_running locklessly. Use READ_ONCE() there. Add corresponding WRITE_ONCE() to netlink_dump() and __netlink_dump_start() syzbot reported: BUG: KCSAN: data-race in __netlink_dump_start / netlink_recvmsg write to 0xffff88813ea4db59 of 1 bytes by task 28219 on cpu 0: __netlink_dump_start+0x3af/0x4d0 net/netlink/af_netlink.c:2399 netlink_dump_start include/linux/netlink.h:308 [inline] rtnetlink_rcv_msg+0x70f/0x8c0 net/core/rtnetlink.c:6130 netlink_rcv_skb+0x126/0x220 net/netlink/af_netlink.c:2577 rtnetlink_rcv+0x1c/0x20 net/core/rtnetlink.c:6192 netlink_unicast_kernel net/netlink/af_netlink.c:1339 [inline] netlink_unicast+0x56f/0x640 net/netlink/af_netlink.c:1365 netlink_sendmsg+0x665/0x770 net/netlink/af_netlink.c:1942 sock_sendmsg_nosec net/socket.c:724 [inline] sock_sendmsg net/socket.c:747 [inline] sock_write_iter+0x1aa/0x230 net/socket.c:1138 call_write_iter include/linux/fs.h:1851 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x463/0x760 fs/read_write.c:584 ksys_write+0xeb/0x1a0 fs/read_write.c:637 __do_sys_write fs/read_write.c:649 [inline] __se_sys_write fs/read_write.c:646 [inline] __x64_sys_write+0x42/0x50 fs/read_write.c:646 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 read to 0xffff88813ea4db59 of 1 bytes by task 28222 on cpu 1: netlink_recvmsg+0x3b4/0x730 net/netlink/af_netlink.c:2022 sock_recvmsg_nosec+0x4c/0x80 net/socket.c:1017 ___sys_recvmsg+0x2db/0x310 net/socket.c:2718 ___sys_recvmsg net/socket.c:2762 [inline] do_recvmmsg+0x2e5/0x710 net/socket.c:2856 __sys_recvmmsg net/socket.c:2935 [inline] __do_sys_recvmmsg net/socket.c:2958 [inline] __se_sys_recvmmsg net/socket.c:2951 [inline] __x64_sys_recvmmsg+0xe2/0x160 net/socket.c:2951 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: 0x00 -> 0x01	N/A	More Details
CVE-2023-53854	In the Linux kernel, the following vulnerability has been resolved: ASoC: mediatek: mt8186: Fix use-after-free in driver remove path When devm runs function in the "remove" path for a device it runs them in the reverse order. That means that if you have parts of your driver that aren't using devm or are using "roll your own" devm w/ devm_add_action_or_reset() you need to keep that in mind. The mt8186 audio driver didn't quite get this right. Specifically, in mt8186_init_clock() it called mt8186_audsys_clk_register() and then went on to call a bunch of other devm function. The caller of mt8186_init_clock() used devm_add_action_or_reset() to call mt8186_deinit_clock() but, because of the intervening devm functions, the order was wrong. Specifically at probe time, the order was: 1. mt8186_audsys_clk_register() 2. afe_priv->clk = devm_kcalloc(...) 3. afe_priv->clk[i] = devm_clk_get(...) At remove time, the order (which should have been 3, 2, 1) was: 1. mt8186_audsys_clk_unregister() 3. Free all of afe_priv->clk[i] 2. Free afe_priv->clk The above seemed to be causing a use-after-free. Luckily, it's easy to fix this by simply using devm more correctly. Let's move the devm_add_action_or_reset() to the right place. In addition to fixing the use-after-free, code inspection shows that this fixes a leak (missing call to mt8186_audsys_clk_unregister()) that would have happened if any of the syscon_regmap_lookup_by_phandle() calls in mt8186_init_clock() had failed.	N/A	More Details
CVE-2023-53855	In the Linux kernel, the following vulnerability has been resolved: net: dsa: ocelot: call dsa_tag_8021q_unregister() under rtnl_lock() on driver remove When the tagging protocol in current use is "ocelot-8021q" and we unbind the driver, we see this splat: $ echo '0000:00:00.2' > /sys/bus/pci/drivers/fsl_enetc/unbind mscc_felix 0000:00:00.5 swp0: left promiscuous mode sja1105 spi2.0: Link is Down DSA: tree 1 torn down mscc_felix 0000:00:00.5 swp2: left promiscuous mode sja1105 spi2.2: Link is Down DSA: tree 3 torn down fsl_enetc 0000:00:00.2 eno2: left promiscuous mode mscc_felix 0000:00:00.5: Link is Down ------------[cut here]------------ RTNL: assertion failed at net/dsa/tag_8021q.c (409) WARNING: CPU: 1 PID: 329 at net/dsa/tag_8021q.c:409 dsa_tag_8021q_unregister+0x12c/0x1a0 Modules linked in: CPU: 1 PID: 329 Comm: bash Not tainted 6.5.0-rc3+ #771 pc : dsa_tag_8021q_unregister+0x12c/0x1a0 lr : dsa_tag_8021q_unregister+0x12c/0x1a0 Call trace: dsa_tag_8021q_unregister+0x12c/0x1a0 felix_tag_8021q_teardown+0x130/0x150 felix_teardown+0x3c/0xd8 dsa_tree_teardown_switches+0xbc/0xe0 dsa_unregister_switch+0x168/0x260 felix_pci_remove+0x30/0x60 pci_device_remove+0x4c/0x100 device_release_driver_internal+0x188/0x288 device_links_unbind_consumers+0xfc/0x138 device_release_driver_internal+0xe0/0x288 device_driver_detach+0x24/0x38 unbind_store+0xd8/0x108 drv_attr_store+0x30/0x50 ---[end trace 0000000000000000]--- ------------[cut here]------------ RTNL: assertion failed at net/8021q/vlan_core.c (376) WARNING: CPU: 1 PID: 329 at net/8021q/vlan_core.c:376 vlan_vid_del+0x1b8/0x1f0 CPU: 1 PID: 329 Comm: bash Tainted: G W 6.5.0-rc3+ #771 pc : vlan_vid_del+0x1b8/0x1f0 lr : vlan_vid_del+0x1b8/0x1f0 dsa_tag_8021q_unregister+0x8c/0x1a0 felix_tag_8021q_teardown+0x130/0x150 felix_teardown+0x3c/0xd8 dsa_tree_teardown_switches+0xbc/0xe0 dsa_unregister_switch+0x168/0x260 felix_pci_remove+0x30/0x60 pci_device_remove+0x4c/0x100 device_release_driver_internal+0x188/0x288 device_links_unbind_consumers+0xfc/0x138 device_release_driver_internal+0xe0/0x288 device_driver_detach+0x24/0x38 unbind_store+0xd8/0x108 drv_attr_store+0x30/0x50 DSA: tree 0 torn down This was somewhat not so easy to spot, because "ocelot-8021q" is not the default tagging protocol, and thus, not everyone who tests the unbinding path may have switched to it beforehand. The default felix_tag_npi_teardown() does not require rtnl_lock() to be held.	N/A	More Details
CVE-2023-53856	In the Linux kernel, the following vulnerability has been resolved: of: overlay: Call of_changeset_init() early When of_overlay_fdt_apply() fails, the changeset may be partially applied, and the caller is still expected to call of_overlay_remove() to clean up this partial state. However, of_overlay_apply() calls of_resolve_phandles() before init_overlay_changeset(). Hence if the overlay fails to apply due to an unresolved symbol, the overlay_changeset.cset.entries list is still uninitialized, and cleanup will crash with a NULL-pointer dereference in overlay_removal_is_ok(). Fix this by moving the call to of_changeset_init() from init_overlay_changeset() to of_overlay_fdt_apply(), where all other early initialization is done.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: bpf: bpf_sk_storage: Fix invalid wait context lockdep report './test_progs -t test_local_storage' reported a splat: [27.137569] ============================== [27.138122] [BUG: Invalid wait		

CVE-2023-53857	context] [27.138650] 6.5.0-03980-gd11ae1b16b0a #247 Tainted: G O [27.139542] ---------- [27.140106] test_progs/1729 is trying to lock: [27.140713] ffff8883ef047b88 (stock_lock){-.-.}-{3:3}, at: local_lock_acquire+0x9/0x130 [27.141834] other info that might help us debug this: [27.142437] context-{5:5} [27.142856] 2 locks held by test_progs/1729: [27.143352] #0: ffffffff84bcd9c0 (rcu_read_lock){....}-{1:3}, at: rcu_lock_acquire+0x4/0x40 [27.144492] #1: ffff888107deb2c0 (&storage->lock){..-.}-{2:2}, at: bpf_local_storage_update+0x39e/0x8e0 [27.145855] stack backtrace: [27.146274] CPU: 0 PID: 1729 Comm: test_progs Tainted: G O 6.5.0-03980-gd11ae1b16b0a #247 [27.147550] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 [27.149127] Call Trace: [27.149490] <TASK> [27.149867] dump_stack_lvl+0x130/0x1d0 [27.152609] dump_stack+0x14/0x20 [27.153131] __lock_acquire+0x1657/0x2220 [27.153677] lock_acquire+0x1b8/0x510 [27.157908] local_lock_acquire+0x29/0x130 [27.159048] obj_cgroup_charge+0xf4/0x3c0 [27.160794] slab_pre_alloc_hook+0x28e/0x2b0 [27.161931] __kmem_cache_alloc_node+0x51/0x210 [27.163557] __kmalloc+0xaa/0x210 [27.164593] bpf_map_kzalloc+0xbc/0x170 [27.165147] bpf_selem_alloc+0x130/0x510 [27.166295] bpf_local_storage_update+0x5aa/0x8e0 [27.167042] bpf_fd_sk_storage_update_elem+0xdb/0x1a0 [27.169199] bpf_map_update_value+0x415/0x4f0 [27.169871] map_update_elem+0x413/0x550 [27.170330] __sys_bpf+0x5e9/0x640 [27.174065] __x64_sys_bpf+0x80/0x90 [27.174568] do_syscall_64+0x48/0xa0 [27.175201] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [27.175932] RIP: 0033:0x7effb40e41ad [27.176357] Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d8 [27.179028] RSP: 002b:00007ffe64c21fc8 EFLAGS: 00000202 ORIG_RAX: 0000000000000141 [27.180088] RAX: ffffffffffffffda RBX: 00007ffe64c22768 RCX: 00007effb40e41ad [27.181082] RDX: 0000000000000020 RSI: 00007ffe64c22008 RDI: 0000000000000002 [27.182030] RBP: 00007ffe64c21ff0 R08: 0000000000000000 R09: 00007ffe64c22788 [27.183038] R10: 0000000000000064 R11: 0000000000000202 R12: 0000000000000000 [27.184006] R13: 00007ffe64c22788 R14: 00007effb42a1000 R15: 0000000000000000 [27.184958] </TASK> It complains about acquiring a local_lock while holding a raw_spin_lock. It means it should not allocate memory while holding a raw_spin_lock since it is not safe for RT. raw_spin_lock is needed because bpf_local_storage supports tracing context. In particular for task local storage, it is easy to get a "current" task PTR_TO_BTF_ID in tracing bpf prog. However, task (and cgroup) local storage has already been moved to bpf mem allocator which can be used after raw_spin_lock. The splat is for the sk storage. For sk (and inode) storage, it has not been moved to bpf mem allocator. Using raw_spin_lock or not, kzalloc(GFP_ATOMIC) could theoretically be unsafe in tracing context. However, the local storage helper requires a verifier accepted sk pointer (PTR_TO_BTF_ID), it is hypothetical if that (mean running a bpf prog in a kzalloc unsafe context and also able to hold a verifier accepted sk pointer) could happen. This patch avoids kzalloc after raw_spin_lock to silent the splat. There is an existing kzalloc before the raw_spin_lock. At that point, a kzalloc is very likely required because a lookup has just been done before. Thus, this patch always does the kzalloc before acq ---truncated---	N/A	More Details
CVE-2023-53858	In the Linux kernel, the following vulnerability has been resolved: tty: serial: samsung_tty: Fix a memory leak in s3c24xx_serial_getclk() in case of error If clk_get_rate() fails, the clk that has just been allocated needs to be freed.	N/A	More Details
CVE-2023-53859	In the Linux kernel, the following vulnerability has been resolved: s390/idle: mark arch_cpu_idle() noinstr linux-next commit ("cpuidle: tracing: Warn about !rcu_is_watching()") adds a new warning which hits on s390's arch_cpu_idle() function: RCU not on for: arch_cpu_idle+0x0/0x28 WARNING: CPU: 2 PID: 0 at include/linux/trace_recursion.h:162 arch_ftrace_ops_list_func+0x24c/0x258 Modules linked in: CPU: 2 PID: 0 Comm: swapper/2 Not tainted 6.2.0-rc6-next-20230202 #4 Hardware name: IBM 8561 T01 703 (z/VM 7.3.0) Krnl PSW : 0404d00180000000 00000000002b55c0 (arch_ftrace_ops_list_func+0x250/0x258) R:0 T:1 IO:0 EX:0 Key:0 M:1 W:0 P:0 AS:3 CC:1 PM:0 RI:0 EA:3 Krnl GPRS: c0000000ffffbfff 0000000080000002 0000000000000026 0000000000000000 0000037ffffe3a28 0000037ffffe3a20 0000000000000000 0000000000000000 0000000000000000 0000000000f4acf6 00000000001044f0 0000037ffffe3cb0 0000000000000000 0000000000000000 00000000002b55bc 0000037ffffe3bb8 Krnl Code: 00000000002b55b0: c02000840051 larl %r2,0000000001335652 00000000002b55b6: c0e5fff512d1 brasl %r14,0000000000157b58 #00000000002b55bc: af000000 mc 0,0 >00000000002b55c0: a7f4ffe7 brc 15,00000000002b558e 00000000002b55c4: 0707 bcr 0,%r7 00000000002b55c6: 0707 bcr 0,%r7 00000000002b55c8: eb6ff0480024 stmg %r6,%r15,72(%r15) 00000000002b55ce: b90400ef lgr %r14,%r15 Call Trace: [<00000000002b55c0>] arch_ftrace_ops_list_func+0x250/0x258 ([<00000000002b55bc>] arch_ftrace_ops_list_func+0x24c/0x258) [<0000000000f5f0fc>] ftrace_common+0x1c/0x20 [<00000000001044f6>] arch_cpu_idle+0x6/0x28 [<0000000000f4acf6>] default_idle_call+0x76/0x128 [<00000000001cc374>] do_idle+0xf4/0x1b0 [<00000000001cc6ce>] cpu_startup_entry+0x36/0x40 [<0000000000119d00>] smp_start_secondary+0x140/0x150 [<0000000000f5d2ae>] restart_int_handler+0x6e/0x90 Mark arch_cpu_idle() noinstr like all other architectures with CONFIG_ARCH_WANTS_NO_INSTR (should) have it to fix this.	N/A	More Details
CVE-2023-53860	In the Linux kernel, the following vulnerability has been resolved: dm: don't attempt to queue IO under RCU protection dm looks up the table for IO based on the request type, with an assumption that if the request is marked REQ_NOWAIT, it's fine to attempt to submit that IO while under RCU read lock protection. This is not OK, as REQ_NOWAIT just means that we should not be sleeping waiting on other IO, it does not mean that we can't potentially schedule. A simple test case demonstrates this quite nicely: int main(int argc, char *argv[]) { struct iovec iov; int fd; fd = open("/dev/dm-0", O_RDONLY | O_DIRECT); posix_memalign(&iov.iov_base, 4096, 4096); iov.iov_len = 4096; preadv2(fd, &iov, 1, 0, RWF_NOWAIT); return 0; } which will instantly spew: BUG: sleeping function called from invalid context at include/linux/sched/mm.h:306 in_atomic(): 0, irqs_disabled(): 0, non_block: 0, pid: 5580, name: dm-nowait preempt_count: 0, expected: 0 RCU nest depth: 1, expected: 0 INFO: lockdep is turned off. CPU: 7 PID: 5580 Comm: dm-nowait Not tainted 6.6.0-rc1-g39956d2dcd81 #132 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x11d/0x1b0 __might_resched+0x3c3/0x5e0 ? preempt_count_sub+0x150/0x150 mempool_alloc+0x1e2/0x390 ? mempool_resize+0x7d0/0x7d0 ? lock_sync+0x190/0x190 ? lock_release+0x4b7/0x670 ? internal_get_user_pages_fast+0x868/0x2d40 bio_alloc_bioset+0x417/0x8c0 ? bvec_alloc+0x200/0x200 ? internal_get_user_pages_fast+0xb8c/0x2d40 bio_alloc_clone+0x53/0x100 dm_submit_bio+0x27f/0x1a20 ? lock_release+0x4b7/0x670 ? blk_try_enter_queue+0x1a0/0x4d0 ? dm_dax_direct_access+0x260/0x260 ? rcu_is_watching+0x12/0xb0 ? blk_try_enter_queue+0x1cc/0x4d0 __submit_bio+0x239/0x310 ? __bio_queue_enter+0x700/0x700 ? kvm_clock_get_cycles+0x40/0x60 ? ktime_get+0x285/0x470 submit_bio_noacct_nocheck+0x4d9/0xb80 ? should_fail_request+0x80/0x80 ? preempt_count_sub+0x150/0x150 ? lock_release+0x4b7/0x670 ? __bio_add_page+0x143/0x2d0 ? iov_iter_revert+0x27/0x360 submit_bio_noacct+0x53e/0x1b30 submit_bio_wait+0x10a/0x230 ? submit_bio_wait_endio+0x40/0x40 __blkdev_direct_IO_simple+0x4f8/0x780 ? blkdev_bio_end_io+0x4c0/0x4c0 ? stack_trace_save+0x90/0xc0 ? __bio_clone+0x3c0/0x3c0 ? lock_release+0x4b7/0x670 ? lock_sync+0x190/0x190 ? atime_needs_update+0x3bf/0x7e0 ? timestamp_truncate+0x21b/0x2d0 ? inode_owner_or_capable+0x240/0x240 blkdev_direct_IO.part.0+0x84a/0x1810 ? rcu_is_watching+0x12/0xb0 ? lock_release+0x4b7/0x670 ? blkdev_read_iter+0x40d/0x530 ? reacquire_held_locks+0x4e0/0x4e0 ? __blkdev_direct_IO_simple+0x780/0x780 ? rcu_is_watching+0x12/0xb0 ? __mark_inode_dirty+0x297/0xd50 ? preempt_count_add+0x72/0x140 blkdev_read_iter+0x2a4/0x530 do_iter_readv_writev+0x2f2/0x3c0 ? generic_copy_file_range+0x1d0/0x1d0 ? fsnotify_perm.part.0+0x25d/0x630 ? security_file_permission+0xd8/0x100 do_iter_read+0x31b/0x880 ? import_iovec+0x10b/0x140 vfs_readv+0x12d/0x1a0 ? vfs_iter_read+0xb0/0xb0 ? rcu_is_watching+0x12/0xb0 ? rcu_is_watching+0x12/0xb0 ? lock_release+0x4b7/0x670 do_preadv+0x1b3/0x260 ? do_readv+0x370/0x370 __x64_sys_preadv2+0xef/0x150 do_syscall_64+0x39/0xb0 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7f5af41ad806 Code: 41 54 41 89 fc 55 44 89 c5 53 48 89 cb 48 83 ec 18 80 3d e4 dd 0d 00 00 74 7a 45 89 c1 49 89 ca 45 31 c0 b8 47 01 00 00 0f 05 <48> 3d 00 f0 ff ff 0f 87 be 00 00 00 48 85 c0 79 4a 48 8b 0d da 55 RSP: 002b:00007ffd3145c7f0 EFLAGS: 00000246 ORIG_RAX: 0000000000000147 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f5af41ad806 RDX: 0000000000000001 RSI: 00007ffd3145c850 RDI: 0000000000000003 RBP: 0000000000000008 R08: 0000000000000000 R09: 0000000000000008 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000003 R13: 00007ffd3145c850 R14: 000055f5f0431dd8 R15: 0000000000000001 </TASK> where in fact it is ---truncated---	N/A	More Details
CVE-			

2023-53861	In the Linux kernel, the following vulnerability has been resolved: ext4: correct grp validation in ext4_mb_good_group Group corruption check will access memory of grp and will trigger kernel crash if grp is NULL. So do NULL check before corruption check.	N/A	More Details
CVE-2023-53863	In the Linux kernel, the following vulnerability has been resolved: netlink: do not hard code device address lenth in fdb dumps syzbot reports that some netdev devices do not have a six bytes address [1] Replace ETH_ALEN by dev->addr_len. [1] (Case of a device where dev->addr_len = 4) BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copyout+0xb8/0x100 lib/iov_iter.c:169 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copyout+0xb8/0x100 lib/iov_iter.c:169 _copy_to_iter+0x6d8/0x1d00 lib/iov_iter.c:536 copy_to_iter include/linux/uio.h:206 [inline] simple_copy_to_iter+0x68/0xa0 net/core/datagram.c:513 __skb_datagram_iter+0x123/0xdc0 net/core/datagram.c:419 skb_copy_datagram_iter+0x5c/0x200 net/core/datagram.c:527 skb_copy_datagram_msg include/linux/skbuff.h:3960 [inline] netlink_recvmsg+0x4ae/0x15a0 net/netlink/af_netlink.c:1970 sock_recvmsg_nosec net/socket.c:1019 [inline] sock_recvmsg net/socket.c:1040 [inline] ____sys_recvmsg+0x283/0x7f0 net/socket.c:2722 ___sys_recvmsg+0x223/0x840 net/socket.c:2764 do_recvmmsg+0x4f9/0xfd0 net/socket.c:2858 __sys_recvmmsg net/socket.c:2937 [inline] __do_sys_recvmmsg net/socket.c:2960 [inline] __se_sys_recvmmsg net/socket.c:2953 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:2953 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 Uninit was stored to memory at: __nla_put lib/nlattr.c:1009 [inline] nla_put+0x1c6/0x230 lib/nlattr.c:1067 nlmsg_populate_fdb_fill+0x2b8/0x600 net/core/rtnetlink.c:4071 nlmsg_populate_fdb net/core/rtnetlink.c:4418 [inline] ndo_dflt_fdb_dump+0x616/0x840 net/core/rtnetlink.c:4456 rtnl_fdb_dump+0x14ff/0x1fc0 net/core/rtnetlink.c:4629 netlink_dump+0x9d1/0x1310 net/netlink/af_netlink.c:2268 netlink_recvmsg+0xc5c/0x15a0 net/netlink/af_netlink.c:1995 sock_recvmsg_nosec+0x7a/0x120 net/socket.c:1019 ____sys_recvmsg+0x664/0x7f0 net/socket.c:2720 ___sys_recvmsg+0x223/0x840 net/socket.c:2764 do_recvmmsg+0x4f9/0xfd0 net/socket.c:2858 __sys_recvmmsg net/socket.c:2937 [inline] __do_sys_recvmmsg net/socket.c:2960 [inline] __se_sys_recvmmsg net/socket.c:2953 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:2953 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 Uninit was created at: slab_post_alloc_hook+0x12d/0xb60 mm/slab.h:716 slab_alloc_node mm/slub.c:3451 [inline] __kmem_cache_alloc_node+0x4ff/0x8b0 mm/slub.c:3490 kmalloc_trace+0x51/0x200 mm/slab_common.c:1057 kmalloc include/linux/slab.h:559 [inline] __hw_addr_create net/core/dev_addr_lists.c:60 [inline] __hw_addr_add_ex+0x2e5/0x9e0 net/core/dev_addr_lists.c:118 __dev_mc_add net/core/dev_addr_lists.c:867 [inline] dev_mc_add+0x9a/0x130 net/core/dev_addr_lists.c:885 igmp6_group_added+0x267/0xbc0 net/ipv6/mcast.c:680 ipv6_mc_up+0x296/0x3b0 net/ipv6/mcast.c:2754 ipv6_mc_remap+0x1e/0x30 net/ipv6/mcast.c:2708 addrconf_type_change net/ipv6/addrconf.c:3731 [inline] addrconf_notify+0x4d3/0x1d90 net/ipv6/addrconf.c:3699 notifier_call_chain kernel/notifier.c:93 [inline] raw_notifier_call_chain+0xe4/0x430 kernel/notifier.c:461 call_netdevice_notifiers_info net/core/dev.c:1935 [inline] call_netdevice_notifiers_extack net/core/dev.c:1973 [inline] call_netdevice_notifiers+0x1ee/0x2d0 net/core/dev.c:1987 bond_enslave+0xccd/0x53f0 drivers/net/bonding/bond_main.c:1906 do_set_master net/core/rtnetlink.c:2626 [inline] rtnl_newlink_create net/core/rtnetlink.c:3460 [inline] __rtnl_newlink net/core/rtnetlink.c:3660 [inline] rtnl_newlink+0x378c/0x40e0 net/core/rtnetlink.c:3673 rtnetlink_rcv_msg+0x16a6/0x1840 net/core/rtnetlink.c:6395 netlink_rcv_skb+0x371/0x650 net/netlink/af_netlink.c:2546 rtnetlink_rcv+0x34/0x40 net/core/rtnetlink.c:6413 netlink_unicast_kernel net/netlink/af_netlink.c:1339 [inline] netlink_unicast+0xf28/0x1230 net/netlink/af_ ---truncated---	N/A	More Details
CVE-2025-12195	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS's CLI could allow an authenticated privileged user to execute arbitrary code via specially crafted IPSec configuration CLI commands.This vulnerability affects Fireware OS 11.0 up to and including 11.12.4+541730, 12.0 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2023-53864	In the Linux kernel, the following vulnerability has been resolved: drm/mxsfb: Disable overlay plane in mxsfb_plane_overlay_atomic_disable() When disabling overlay plane in mxsfb_plane_overlay_atomic_update(), overlay plane's framebuffer pointer is NULL. So, dereferencing it would cause a kernel Oops(NULL pointer dereferencing). Fix the issue by disabling overlay plane in mxsfb_plane_overlay_atomic_disable() instead.	N/A	More Details
CVE-2023-53865	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix warning when putting transaction with qgroups enabled after abort If we have a transaction abort with qgroups enabled we get a warning triggered when doing the final put on the transaction, like this: [552.6789] ------------[cut here]------------ [552.6815] WARNING: CPU: 4 PID: 81745 at fs/btrfs/transaction.c:144 btrfs_put_transaction+0x123/0x130 [btrfs] [552.6817] Modules linked in: btrfs blake2b_generic xor (...) [552.6819] CPU: 4 PID: 81745 Comm: btrfs-transacti Tainted: G W 6.4.0-rc6-btrfs-next-134+ #1 [552.6819] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-0-gea1b7a073390-prebuilt.qemu.org 04/01/2014 [552.6819] RIP: 0010:btrfs_put_transaction+0x123/0x130 [btrfs] [552.6821] Code: bd a0 01 00 (...) [552.6821] RSP: 0018:ffffa168c0527e28 EFLAGS: 00010286 [552.6821] RAX: ffff936042caed00 RBX: ffff93604a3eb448 RCX: 0000000000000000 [552.6821] RDX: ffff93606421b028 RSI: ffffffff92ff0878 RDI: ffff93606421b010 [552.6821] RBP: ffff93606421b000 R08: 0000000000000000 R09: ffffa168c0d07c20 [552.6821] R10: 0000000000000000 R11: ffff93608dc52950 R12: ffffa168c0527e70 [552.6821] R13: ffff93606421b000 R14: ffff93604a3eb420 R15: ffff93606421b028 [552.6821] FS: 0000000000000000(0000) GS:ffff93675fb00000(0000) knlGS:0000000000000000 [552.6821] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [552.6821] CR2: 0000558ad262b000 CR3: 000000014feda005 CR4: 0000000000370ee0 [552.6822] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [552.6822] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [552.6822] Call Trace: [552.6822] <TASK> [552.6822] ? __warn+0x80/0x130 [552.6822] ? btrfs_put_transaction+0x123/0x130 [btrfs] [552.6824] ? report_bug+0x1f4/0x200 [552.6824] ? handle_bug+0x42/0x70 [552.6824] ? exc_invalid_op+0x14/0x70 [552.6824] ? asm_exc_invalid_op+0x16/0x20 [552.6824] ? btrfs_put_transaction+0x123/0x130 [btrfs] [552.6826] btrfs_cleanup_transaction+0xe7/0x5e0 [btrfs] [552.6828] ? _raw_spin_unlock_irqrestore+0x23/0x40 [552.6828] ? try_to_wake_up+0x94/0x5e0 [552.6828] ? __pfx_process_timeout+0x10/0x10 [552.6828] transaction_kthread+0x103/0x1d0 [btrfs] [552.6830] ? __pfx_transaction_kthread+0x10/0x10 [btrfs] [552.6832] kthread+0xee/0x120 [552.6832] ? __pfx_kthread+0x10/0x10 [552.6832] ret_from_fork+0x29/0x50 [552.6832] </TASK> [552.6832] ---[end trace 0000000000000000]--- This corresponds to this line of code: void btrfs_put_transaction(struct btrfs_transaction *transaction) { (...) WARN_ON(!RB_EMPTY_ROOT(&transaction->delayed_refs.dirty_extent_root)); (...) } The warning happens because btrfs_qgroup_destroy_extent_records(), called in the transaction abort path, we free all entries from the rbtree "dirty_extent_root" with rbtree_postorder_for_each_entry_safe(), but we don't actually empty the rbtree - it's still pointing to nodes that were freed. So set the rbtree's root node to NULL to avoid this warning (assign RB_ROOT).	N/A	More Details
CVE-2023-53866	In the Linux kernel, the following vulnerability has been resolved: ASoC: soc-compress: Reposition and add pcm_mutex If panic_on_warn is set and compress stream(DPCM) is started, then kernel panic occurred because card->pcm_mutex isn't held appropriately. In the following functions, warning were issued at this line "snd_soc_dpcm_mutex_assert_held". static int dpcm_be_connect(struct snd_soc_pcm_runtime *fe, struct snd_soc_pcm_runtime *be, int stream) { ... snd_soc_dpcm_mutex_assert_held(fe); ... } void dpcm_be_disconnect(struct snd_soc_pcm_runtime *fe, int stream) { ... snd_soc_dpcm_mutex_assert_held(fe); ... } void snd_soc_runtime_action(struct snd_soc_pcm_runtime *rtd, int stream, int action) { ... snd_soc_dpcm_mutex_assert_held(rtd); ... } int dpcm_dapm_stream_event(struct snd_soc_pcm_runtime *fe, int dir, int event) { ... snd_soc_dpcm_mutex_assert_held(fe); ... } These functions are called by soc_compr_set_params_fe, soc_compr_open_fe and soc_compr_free_fe without pcm_mutex locking. And this is call stack. [414.527841][T2179] pc : dpcm_process_paths+0x5a4/0x750 [414.527848][T2179] lr : dpcm_process_paths+0x37c/0x750 [414.527945][T2179] Call trace: [414.527949][T2179] dpcm_process_paths+0x5a4/0x750 [414.527955][T2179] soc_compr_open_fe+0xb0/0x2cc [414.527972][T2179] snd_compr_open+0x180/0x248 [414.527981][T2179] snd_open+0x15c/0x194 [414.528003][T2179] chrdev_open+0x1b0/0x220 [414.528023][T2179] do_dentry_open+0x30c/0x594 [414.528045][T2179] vfs_open+0x34/0x44 [414.528053][T2179] path_openat+0x914/0xb08 [414.528062][T2179] do_filp_open+0xc0/0x170 [414.528068][T2179] do_sys_openat2+0x94/0x18c [	N/A	More Details

	414.528076][T2179] __arm64_sys_openat+0x78/0xa4 [414.528084][T2179] invoke_syscall+0x48/0x10c [414.528094][T2179] el0_svc_common+0xbc/0x104 [414.528099][T2179] do_el0_svc+0x34/0xd8 [414.528103][T2179] el0_svc+0x34/0xc4 [414.528125][T2179] el0t_64_sync_handler+0x8c/0xfc [414.528133][T2179] el0t_64_sync+0x1a0/0x1a4 [414.528142][T2179] Kernel panic - not syncing: panic_on_warn set ... So, I reposition and add pcm_mutex to resolve lockdep error.		
CVE-2024-38798	EDK2 contains a vulnerability in BIOS where an attacker may cause “Exposure of Sensitive Information to an Unauthorized Actor” by local access. Successful exploitation of this vulnerability will lead to possible information disclosure or escalation of privilege and impact Confidentiality.	N/A	More Details
CVE-2025-13937	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (ConnectWise Technology Integration module) allows Stored XSS.This issue affects Fireware OS 12.4 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-13936	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (Tigerpaw Technology Integration module) allows Stored XSS.This issue affects Fireware OS 12.4 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-13932	The SolisCloud API suffers from a Broken Access Control vulnerability, specifically an Insecure Direct Object Reference (IDOR), where any authenticated user can access detailed data of any plant by altering the plant_id in the request.	N/A	More Details
CVE-2025-12986	When a WF200/WGM160P device is configured to operate as an Access Point, it may be vulnerable to a denial of service triggered by a malformed packet. The device may recover automatically or require a hard reset.	N/A	More Details
CVE-2025-12196	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS's CLI could allow an authenticated privileged user to execute arbitrary code via a specially crafted CLI command.This vulnerability affects Fireware OS 12.0 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-14327	Spoofing issue in the Downloads Panel component. This vulnerability affects Firefox < 146.	N/A	More Details
CVE-2025-66555	AirKeyboard iOS App 1.0.5 contains a missing authentication vulnerability that allows unauthenticated attackers to type arbitrary keystrokes directly into the victim's iOS device in real-time without user interaction, resulting in full remote input control.	N/A	More Details
CVE-2025-66479	Anthropic Sandbox Runtime is a lightweight sandboxing tool for enforcing filesystem and network restrictions on arbitrary processes at the OS level, without requiring a container. Prior to 0.0.16, due to a bug in sandboxing logic, sandbox-runtime did not properly enforce a network sandbox if the sandbox policy did not configure any allowed domains. This could allow sandboxed code to make network requests outside of the sandbox. A patch for this was released in v0.0.16.	N/A	More Details
CVE-2025-49347	Cross-Site Request Forgery (CSRF) vulnerability in Jupitercow WP sIFR wp-sifr allows Stored XSS.This issue affects WP sIFR: from n/a through <= 0.6.8.1.	N/A	More Details
CVE-2023-53735	WEBIGniter 28.7.23 contains a cross-site scripting vulnerability in the user creation process that allows unauthenticated attackers to execute malicious JavaScript code, enabling potential XSS attacks.	N/A	More Details
CVE-2023-53734	dawa-pharma-1.0 allows unauthenticated attackers to execute SQL queries on the server, allowing them to access sensitive information and potentially gain administrative access.	N/A	More Details
CVE-2025-13488	Due to a regression introduced in version 3.83.0, a security header is no longer applied to certain user-uploaded content served from repositories. This may allow an authenticated attacker with repository upload privileges to exploit a stored cross-site scripting (XSS) vulnerability with user context.	N/A	More Details
CVE-2025-9127	A vulnerability exists in PX Enterprise whereby sensitive information may be logged under specific conditions.	N/A	More Details
CVE-2025-66516	Critical XXE in Apache Tika tika-core (1.13-3.2.1), tika-pdf-module (2.0.0-3.2.1) and tika-parsers (1.13-1.28.5) modules on all platforms allows an attacker to carry out XML External Entity injection via a crafted XFA file inside of a PDF. This CVE covers the same vulnerability as in CVE-2025-54988. However, this CVE expands the scope of affected packages in two ways. First, while the entrypoint for the vulnerability was the tika-parser-pdf-module as reported in CVE-2025-54988, the vulnerability and its fix were in tika-core. Users who upgraded the tika-parser-pdf-module but did not upgrade tika-core to >= 3.2.2 would still be vulnerable. Second, the original report failed to mention that in the 1.x Tika releases, the PDFParser was in the "org.apache.tika:tika-parsers" module.	N/A	More Details
CVE-2025-40266	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Check the untrusted offset in FF-A memory share Verify the offset to prevent OOB access in the hypervisor FF-A buffer in case an untrusted large enough value [U32_MAX - sizeof(struct ffa_composite_mem_region) + 1, U32_MAX] is set from the host kernel.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: vfat: fix missing sb_min_blocksize() return value checks When emulating an nvme device on qemu with both logical_block_size and physical_block_size set to 8 KiB, but without format, a kernel panic was triggered during the early boot stage while attempting to mount a vfat filesystem. [95553.682035] EXT4-fs (nvme0n1): unable to set blocksize [95553.684326] EXT4-fs (nvme0n1): unable to set blocksize [95553.686501] EXT4-fs (nvme0n1): unable to set blocksize [95553.696448] ISOFS: unsupported/invalid hardware sector size 8192 [95553.697117] ------------[cut here]------------ [95553.697567] kernel BUG at fs/buffer.c:1582! [95553.697984] Oops: invalid opcode: 0000 [#1] SMP NOPTI [95553.698602] CPU: 0 UID: 0 PID: 7212 Comm: mount Kdump: loaded Not tainted 6.18.0-rc2+ #38 PREEMPT(voluntary) [95553.699511] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [95553.700534] RIP: 0010:folio_alloc_buffers+0x1bb/0x1c0 [95553.701018] Code: 48 8b 15 e8 93 18 02 65 48 89 35 e0 93 18 02 48 83 c4 10 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff c3 cc cc cc cc <0f> 0b 90 66 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 0f [95553.702648] RSP: 0018:ffffd1b0c676f990 EFLAGS: 00010246 [95553.703132] RAX: ffff8cfc4176d820 RBX: 0000000000508c48 RCX: 0000000000000001 [95553.703805] RDX: 0000000000002000 RSI: 0000000000000000 RDI: 0000000000000000 [95553.704481] RBP: ffffd1b0c676f9c8 R08: 0000000000000000 R09: 0000000000000000 [95553.705148] R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000001 [95553.705816] R13: 0000000000002000 R14: fffff8bc8257e800 R15: 0000000000000000 [95553.706483] FS: 000072ee77315840(0000) GS:ffff8cfdd2c8d000(0000) knlGS:0000000000000000 [95553.707248] CS: 0010 DS: 0000 ES: 0000 CR0:		

CVE-2025-40265	0000000080050033 [95553.707782] CR2: 00007d8f2a9e5a20 CR3: 0000000039d0c006 CR4: 0000000000772ef0 [95553.708439] PKRU: 55555554 [95553.708734] Call Trace: [95553.709015] <TASK> [95553.709266] __getblk_slow+0xd2/0x230 [95553.709641] ? find_get_block_common+0x8b/0x530 [95553.710084] bdev_getblk+0x77/0xa0 [95553.710449] __bread_gfp+0x22/0x140 [95553.710810] fat_fill_super+0x23a/0xfc0 [95553.711216] ? __pfx_setup+0x10/0x10 [95553.711580] ? __pfx_vfat_fill_super+0x10/0x10 [95553.712014] vfat_fill_super+0x15/0x30 [95553.712401] get_tree_bdev_flags+0x141/0x1e0 [95553.712817] get_tree_bdev+0x10/0x20 [95553.713177] vfat_get_tree+0x15/0x20 [95553.713550] vfs_get_tree+0x2a/0x100 [95553.713910] vfs_cmd_create+0x62/0xf0 [95553.714273] __do_sys_fsconfig+0x4e7/0x660 [95553.714669] __x64_sys_fsconfig+0x20/0x40 [95553.715062] x64_sys_call+0x21ee/0x26a0 [95553.715453] do_syscall_64+0x80/0x670 [95553.715816] ? __fs_parse+0x65/0x1e0 [95553.716172] ? fat_parse_param+0x103/0x4b0 [95553.716587] ? vfs_parse_fs_param_source+0x21/0xa0 [95553.717034] ? __do_sys_fsconfig+0x3d9/0x660 [95553.717548] ? __x64_sys_fsconfig+0x20/0x40 [95553.717957] ? x64_sys_call+0x21ee/0x26a0 [95553.718360] ? do_syscall_64+0xb8/0x670 [95553.718734] ? __x64_sys_fsconfig+0x20/0x40 [95553.719141] ? x64_sys_call+0x21ee/0x26a0 [95553.719545] ? do_syscall_64+0xb8/0x670 [95553.719922] ? x64_sys_call+0x1405/0x26a0 [95553.720317] ? do_syscall_64+0xb8/0x670 [95553.720702] ? __x64_sys_close+0x3e/0x90 [95553.721080] ? x64_sys_call+0x1b5e/0x26a0 [95553.721478] ? do_syscall_64+0xb8/0x670 [95553.721841] ? irqentry_exit+0x43/0x50 [95553.722211] ? exc_page_fault+0x90/0x1b0 [95553.722681] entry_SYSCALL_64_after_hwframe+0x76/0x7e [95553.723166] RIP: 0033:0x72ee774f3afe [95553.723562] Code: 73 01 c3 48 8b 0d 0a 33 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 49 89 ca b8 af 01 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d da 32 0f 00 f7 d8 64 89 01 48 [95553.725188] RSP: 002b:00007ffe97148978 EFLAGS: 00000246 ORIG_RAX: 00000000000001af [95553.725892] RAX: ffffffffffffffda RBX: ---truncated---	N/A	More Details
CVE-2025-40264	In the Linux kernel, the following vulnerability has been resolved: be2net: pass wrb_params in case of OS2BMC be_insert_vlan_in_pkt() is called with the wrb_params argument being NULL at be_send_pkt_to_bmc() call site. This may lead to dereferencing a NULL pointer when processing a workaround for specific packet, as commit bc0c3405abbb ("be2net: fix a Tx stall bug caused by a specific ipv6 packet") states. The correct way would be to pass the wrb_params from be_xmit().	N/A	More Details
CVE-2025-49341	Cross-Site Request Forgery (CSRF) vulnerability in Alex Furr PDF Creator Lite pdf-creator-lite allows Stored XSS.This issue affects PDF Creator Lite: from n/a through <= 1.2.	N/A	More Details
CVE-2025-49348	Missing Authorization vulnerability in Hype Hype pico allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hype: from n/a through <= 1.0.5.	N/A	More Details
CVE-2024-58276	Obi08/Enrollment System 1.0 contains a SQL injection vulnerability in the keyword parameter of /get_subject.php that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can use UNION-based injection to extract sensitive information from the users table including usernames and passwords.	N/A	More Details
CVE-2025-49350	Missing Authorization vulnerability in marcoingraiti Actionwear products sync actionwear-products-sync allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Actionwear products sync: from n/a through <= 2.3.3.	N/A	More Details
CVE-2025-49351	Cross-Site Request Forgery (CSRF) vulnerability in Valentin Agachi Create Posts & Terms create-posts-terms allows Stored XSS.This issue affects Create Posts & Terms: from n/a through <= 1.3.1.	N/A	More Details
CVE-2025-40263	In the Linux kernel, the following vulnerability has been resolved: Input: cros_ec_keyb - fix an invalid memory access If cros_ec_keyb_register_matrix() isn't called (due to `buttons_switches_only`) in cros_ec_keyb_probe(), `ckdev->idev` remains NULL. An invalid memory access is observed in cros_ec_keyb_process() when receiving an EC_MKBP_EVENT_KEY_MATRIX event in cros_ec_keyb_work() in such case. Unable to handle kernel read from unreadable memory at virtual address 0000000000000028 ... x3 : 0000000000000000 x2 : 0000000000000000 x1 : 0000000000000000 x0 : 0000000000000000 Call trace: input_event cros_ec_keyb_work blocking_notifier_call_chain ec_irq_thread It's still unknown about why the kernel receives such malformed event, in any cases, the kernel shouldn't access `ckdev->idev` and friends if the driver doesn't intend to initialize them.	N/A	More Details
CVE-2025-59132	Cross-Site Request Forgery (CSRF) vulnerability in Badi Jones Duplicate Content Cure duplicate-content-cure allows Cross Site Request Forgery.This issue affects Duplicate Content Cure: from n/a through <= 1.0.	N/A	More Details
CVE-2025-5469	Uncontrolled Search Path Element vulnerability in Yandex Messenger on MacOS allows Search Order Hijacking.This issue affects Telemost: before 2.245	N/A	More Details
CVE-2025-5470	Uncontrolled Search Path Element vulnerability in Yandex Disk on MacOS allows Search Order Hijacking.This issue affects Disk: before 3.2.45.3275.	N/A	More Details
CVE-2025-5471	Uncontrolled Search Path Element vulnerability in Yandex Telemost on MacOS allows Search Order Hijacking.This issue affects Telemost: before 2.19.1.	N/A	More Details
CVE-2025-61074	A stored Cross Site Scripting (XSS) vulnherability in the bulletin board (SchwarzeBrett) in adata Software GmbH Mitarbeiter Portal 2.15.2.0 allows remote authenticated users to execute arbitrary JavaScript code in the web browser of other users via manipulation of the 'Inhalt' parameter of the '/SchwarzeBrett/Nachrichten/CreateNachricht' or '/SchwarzeBrett/Nachrichten/EditNachricht/' requests.	N/A	More Details
CVE-2025-61075	Multiple Incorrect Access Control vulnerabilities in adata Software GmbH Mitarbeiterportal 2.15.2.0 allow remote authenticated, low-privileged users to carry out administrative functions and manipulate data of other users via unauthorized API calls.	N/A	More Details
CVE-2024-58275	Easywall 0.3.1 allows authenticated remote command execution via a command injection vulnerability in the /ports-save endpoint that suffers from a parameter injection flaw. Attackers can inject shell metacharacters to execute arbitrary commands on the server.	N/A	More Details
CVE-2024-58277	R Radio Network FM Transmitter 1.07 allows unauthenticated attackers to access the admin user's password through the system.cgi endpoint, enabling authentication bypass and FM station setup access.	N/A	More Details
CVE-2025-14330	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 146 and Firefox ESR < 140.6.	N/A	More Details

CVE-2025-40333	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix infinite loop in __insert_extent_tree() When we get wrong extent info data, and look up extent_node in rb tree, it will cause infinite loop (CONFIG_F2FS_CHECK_FS=n). Avoiding this by return NULL and print some kernel messages in that case.	N/A	More Details
CVE-2025-27935	The OTP Integration Kit for PingFederate fails to enforce HTTP method validation and state validation properly. The server advances the authentication state without verifying the OTP, thereby bypassing multi-factor authentication.	N/A	More Details
CVE-2024-58278	perl2exe <= V30.10C contains an arbitrary code execution vulnerability that allows local authenticated attackers to execute malicious scripts. Attackers can control the 0th argument of packed executables to execute another executable, allowing them to bypass restrictions and gain unauthorized access.	N/A	More Details
CVE-2025-2296	EDK2 contains a vulnerability in BIOS where an attacker may cause “ Improper Input Validation” by local access. Successful exploitation of this vulnerability could alter control flow in unexpected ways, potentially allowing arbitrary command execution and impacting Confidentiality, Integrity, and Availability.	N/A	More Details
CVE-2025-40327	In the Linux kernel, the following vulnerability has been resolved: perf/core: Fix system hang caused by cpu-clock usage cpu-clock usage by the async-profiler tool can trigger a system hang, which got bisected back to the following commit by Octavia Togami: 18dbcbfabfff ("perf: Fix the POLL_HUP delivery breakage") causes this issue The root cause of the hang is that cpu-clock is a special type of SW event which relies on hrtimers. The __perf_event_overflow() callback is invoked from the hrtimer handler for cpu-clock events, and __perf_event_overflow() tries to call cpu_clock_event_stop() to stop the event, which calls htimer_cancel() to cancel the hrtimer. But that's a recursion into the hrtimer code from a hrtimer handler, which (unsurprisingly) deadlocks. To fix this bug, use hrtimer_try_to_cancel() instead, and set the PERF_HES_STOPPED flag, which causes perf_swevent_hrtimer() to stop the event once it sees the PERF_HES_STOPPED flag. [mingo: Fixed the comments and improved the changelog.]	N/A	More Details
CVE-2025-40328	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in smb2_close_cached_fid() find_or_create_cached_dir() could grab a new reference after kref_put() had seen the refcount drop to zero but before cfid_list_lock is acquired in smb2_close_cached_fid(), leading to use-after-free. Switch to kref_put_lock() so cfid_release() is called with cfid_list_lock held, closing that gap.	N/A	More Details
CVE-2025-40329	In the Linux kernel, the following vulnerability has been resolved: drm/sched: Fix deadlock in drm_sched_entity_kill_jobs_cb The Mesa issue referenced below pointed out a possible deadlock: [1231.611031] Possible interrupt unsafe locking scenario: [1231.611033] CPU0 CPU1 [1231.611034] ---- ---- [1231.611035] lock(&xa->xa_lock#17); [1231.611038] local_irq_disable(); [1231.611039] lock(&fence->lock); [1231.611041] lock(&xa->xa_lock#17); [1231.611044] <Interrupt> [1231.611045] lock(&fence->lock); [1231.611047] *** DEADLOCK *** In this example, CPU0 would be any function accessing job->dependencies through the xa_* functions that don't disable interrupts (eg: drm_sched_job_add_dependency(), drm_sched_entity_kill_jobs_cb()). CPU1 is executing drm_sched_entity_kill_jobs_cb() as a fence signalling callback so in an interrupt context. It will deadlock when trying to grab the xa_lock which is already held by CPU0. Replacing all xa_* usage by their xa_*_irq counterparts would fix this issue, but Christian pointed out another issue: dma_fence_signal takes fence.lock and so does dma_fence_add_callback. dma_fence_signal() // locks f1.lock -> drm_sched_entity_kill_jobs_cb() -> foreach dependencies -> dma_fence_add_callback() // locks f2.lock This will deadlock if f1 and f2 share the same spinlock. To fix both issues, the code iterating on dependencies and re-arming them is moved out to drm_sched_entity_kill_jobs_work(). [phasta: commit message nits]	N/A	More Details
CVE-2025-40330	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Shutdown FW DMA in bnxt_shutdown() The netif_close() call in bnxt_shutdown() only stops packet DMA. There may be FW DMA for trace logging (recently added) that will continue. If we kexec to a new kernel, the DMA will corrupt memory in the new kernel. Add bnxt_hwrm_func_drv_unrgtr() to unregister the driver from the FW. This will stop the FW DMA. In case the call fails, call pcie_flr() to reset the function and stop the DMA.	N/A	More Details
CVE-2025-40331	In the Linux kernel, the following vulnerability has been resolved: sctp: Prevent TOCTOU out-of-bounds write For the following path not holding the sock lock, sctp_diag_dump() -> sctp_for_each_endpoint() -> sctp_ep_dump() make sure not to exceed bounds in case the address list has grown between buffer allocation (time-of-check) and write (time-of-use).	N/A	More Details
CVE-2025-40332	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix mmap write lock not release If mmap write lock is taken while draining retry fault, mmap write lock is not released because svm_range_restore_pages calls mmap_read_unlock then returns. This causes deadlock and system hangs later because mmap read or write lock cannot be taken. Downgrade mmap write lock to read lock if draining retry fault fix this bug.	N/A	More Details
CVE-2025-40334	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate userq buffer virtual address and size It needs to validate the userq object virtual address to determine whether it is residented in a valid vm mapping.	N/A	More Details
CVE-2025-40344	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Disable periods-elapsed work when closing PCM avs_dai_fe_shutdown() handles the shutdown procedure for HOST HDAudio stream while period-elapsed work services its IRQs. As the former frees the DAI's private context, these two operations shall be synchronized to avoid slab-use-after-free or worse errors.	N/A	More Details
CVE-2025-40335	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate userq input args This will help on validating the userq input args, and rejecting for the invalid userq request at the IOCTLs first place.	N/A	More Details
CVE-2025-40336	In the Linux kernel, the following vulnerability has been resolved: drm/gpusvm: fix hmm_pfn_to_map_order() usage Handle the case where the hmm range partially covers a huge page (like 2M), otherwise we can potentially end up doing something nasty like mapping memory which is outside the range, and maybe not even mapped by the mm. Fix is based on the xe userptr code, which in a future patch will directly use gpusvm, so needs alignment here. v2: - Add kernel-doc (Matt B) - s/fls/ilog2/ (Thomas)	N/A	More Details
CVE-2025-40337	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: Correctly handle Rx checksum offload errors The stmmac_rx function would previously set skb->ip_summed to CHECKSUM_UNNECESSARY if hardware checksum offload (CoE) was enabled and the packet was of a known IP ethertype. However, this logic failed to check if the hardware had actually reported a checksum error. The hardware status, indicating a header or payload checksum failure, was being ignored at this stage. This could cause corrupt packets to be passed up the network stack as valid. This patch corrects the logic by checking the `csum_none` status flag, which is set when the hardware reports a checksum error. If this flag is set, skb->ip_summed is now correctly set to CHECKSUM_NONE, ensuring the kernel's network stack will perform its own validation and properly handle the corrupt packet.	N/A	More Details
CVE-2025-40338	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: avs: Do not share the name pointer between components By sharing 'name' directly, tearing down components may lead to use-after-free errors. Duplicate the name to avoid that. At the same time, update the order of operations - since commit cee28113db17 ("ASoC: dmaengine_pcm: Allow passing component name via config") the framework does not override component->name if set before invoking the initializer.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix nullptr err of vm_handle_moved If a amdgpu_bo_va is fpriv->prt_va, the bo of this one is always NULL. So, such kind of amdgpu_bo_va should be updated separately before	N/A	More

40339	amdgpu_vm_handle_moved.		Details
CVE-2025-40340	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix oops in xe_gem_fault when running core_hotunplug test. I saw an oops in xe_gem_fault when running the xe-fast-feedback testlist against the realtime kernel without debug options enabled. The panic happens after core_hotunplug unbind-rebind finishes. Presumably what happens is that a process mmaps, unlocks because of the FAULT_FLAG_RETRY_NOWAIT logic, has no process memory left, causing ttm_bo_vm_dummy_page() to return VM_FAULT_NOPAGE, since there was nothing left to populate, and then oopses in "mem_type_is_vram(tbo->resource->mem_type)" because tbo->resource is NULL. It's convoluted, but fits the data and explains the oops after the test exits.	N/A	More Details
CVE-2025-40341	In the Linux kernel, the following vulnerability has been resolved: futex: Don't leak robust_list pointer on exec race sys_get_robust_list() and compat_get_robust_list() use ptrace_may_access() to check if the calling task is allowed to access another task's robust_list pointer. This check is racy against a concurrent exec() in the target process. During exec(), a task may transition from a non-privileged binary to a privileged one (e.g., setuid binary) and its credentials/memory mappings may change. If get_robust_list() performs ptrace_may_access() before this transition, it may erroneously allow access to sensitive information after the target becomes privileged. A racy access allows an attacker to exploit a window during which ptrace_may_access() passes before a target process transitions to a privileged state via exec(). For example, consider a non-privileged task T that is about to execute a setuid-root binary. An attacker task A calls get_robust_list(T) while T is still unprivileged. Since ptrace_may_access() checks permissions based on current credentials, it succeeds. However, if T begins exec immediately afterwards, it becomes privileged and may change its memory mappings. Because get_robust_list() proceeds to access T->robust_list without synchronizing with exec() it may read user-space pointers from a now-privileged process. This violates the intended post-exec access restrictions and could expose sensitive memory addresses or be used as a primitive in a larger exploit chain. Consequently, the race can lead to unauthorized disclosure of information across privilege boundaries and poses a potential security risk. Take a read lock on signal->exec_update_lock prior to invoking ptrace_may_access() and accessing the robust_list/compat_robust_list. This ensures that the target task's exec state remains stable during the check, allowing for consistent and synchronized validation of credentials.	N/A	More Details
CVE-2025-40342	In the Linux kernel, the following vulnerability has been resolved: nvme-fc: use lock accessing port_state and rport state nvme_fc_unregister_remote removes the remote port on a lport object at any point in time when there is no active association. This races with with the reconnect logic, because nvme_fc_create_association is not taking a lock to check the port_state and atomically increase the active count on the rport.	N/A	More Details
CVE-2025-40343	In the Linux kernel, the following vulnerability has been resolved: nvmet-fc: avoid scheduling association deletion twice When forcefully shutting down a port via the configfs interface, nvmet_port_subsys_drop_link() first calls nvmet_port_del_ctrls() and then nvmet_disable_port(). Both functions will eventually schedule all remaining associations for deletion. The current implementation checks whether an association is about to be removed, but only after the work item has already been scheduled. As a result, it is possible for the first scheduled work item to free all resources, and then for the same work item to be scheduled again for deletion. Because the association list is an RCU list, it is not possible to take a lock and remove the list entry directly, so it cannot be looked up again. Instead, a flag (terminating) must be used to determine whether the association is already in the process of being deleted.	N/A	More Details
CVE-2023-53852	In the Linux kernel, the following vulnerability has been resolved: nvme-core: fix memory leak in dhchap_secret_store Free dhchap_secret in nvme_ctrl_dhchap_secret_store() before we return fix following kmemleack:- unreferenced object 0xffff8886376ea800 (size 64): comm "check", pid 22048, jiffies 4344316705 (age 92.199s) hex dump (first 32 bytes): 44 48 48 43 2d 31 3a 30 30 3a 6e 78 72 35 4b 67 DHHC-1:00:nxr5Kg 75 58 34 75 6f 41 78 73 4a 61 34 63 2f 68 75 4c uX4uoAxsJa4c/huL backtrace: [<0000000030ce5d4b>] __kmalloc+0x4b/0x130 [<000000009be1cdc1>] nvme_ctrl_dhchap_secret_store+0x8f/0x160 [nvme_core] [<00000000ac06c96a>] kernfs_fop_write_iter+0x12b/0x1c0 [<00000000437e7ced>] vfs_write+0x2ba/0x3c0 [<00000000f9491baf>] ksys_write+0x5f/0xe0 [<000000001c46513d>] do_syscall_64+0x3b/0x90 [<00000000ecf348fe>] entry_SYSCALL_64_after_hwframe+0x72/0xdc unreferenced object 0xffff8886376eaf00 (size 64): comm "check", pid 22048, jiffies 4344316736 (age 92.168s) hex dump (first 32 bytes): 44 48 48 43 2d 31 3a 30 30 3a 6e 78 72 35 4b 67 DHHC-1:00:nxr5Kg 75 58 34 75 6f 41 78 73 4a 61 34 63 2f 68 75 4c uX4uoAxsJa4c/huL backtrace: [<0000000030ce5d4b>] __kmalloc+0x4b/0x130 [<000000009be1cdc1>] nvme_ctrl_dhchap_secret_store+0x8f/0x160 [nvme_core] [<00000000ac06c96a>] kernfs_fop_write_iter+0x12b/0x1c0 [<00000000437e7ced>] vfs_write+0x2ba/0x3c0 [<00000000f9491baf>] ksys_write+0x5f/0xe0 [<000000001c46513d>] do_syscall_64+0x3b/0x90 [<00000000ecf348fe>] entry_SYSCALL_64_after_hwframe+0x72/0xdc	N/A	More Details
CVE-2023-53850	In the Linux kernel, the following vulnerability has been resolved: iavf: use internal state to free traffic IRQs If the system tries to close the netdev while iavf_reset_task() is running, __LINK_STATE_START will be cleared and netif_running() will return false in iavf_reinit_interrupt_scheme(). This will result in iavf_free_traffic_irqs() not being called and a leak as follows: [7632.489326] remove_proc_entry: removing non-empty directory 'irq/999', leaking at least 'iavf-enp24s0f0v0-TxRx-0' [7632.490214] WARNING: CPU: 0 PID: 10 at fs/proc/generic.c:718 remove_proc_entry+0x19b/0x1b0 is shown when pci_disable_msix() is later called. Fix by using the internal adapter state. The traffic IRQs will always exist if state == __IAVF_RUNNING.	N/A	More Details
CVE-2023-53780	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix FCLK pstate change underflow [Why] Currently we set FCLK p-state change watermark calculated based on dummy p-state latency when UCLK p-state is not supported [How] Calculate FCLK p-state change watermark based on on FCLK pstate change latency in case UCLK p-state is not supported	N/A	More Details
CVE-2023-53849	In the Linux kernel, the following vulnerability has been resolved: drm/msm: fix workqueue leak on bind errors Make sure to destroy the workqueue also in case of early errors during bind (e.g. a subcomponent failing to bind). Since commit c3b790ea07a1 ("drm: Manage drm_mode_config_init with drmm_") the mode config will be freed when the drm device is released also when using the legacy interface, but add an explicit cleanup for consistency and to facilitate backporting. Patchwork: https://patchwork.freedesktop.org/patch/525093/	N/A	More Details
CVE-2023-53805	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-53806	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: populate subvp cmd info only for the top pipe [Why] System restart observed while changing the display resolution to 8k with extended mode. Sytem restart was caused by a page fault. [How] When the driver populates subvp info it did it for both the pipes using vblank which caused an outof bounds array access causing the page fault. added checks to allow the top pipe only to fix this issue.	N/A	More Details
CVE-2023-53807	In the Linux kernel, the following vulnerability has been resolved: clk: clocking-wizard: Fix Oops in clk_wzrd_register_divider() Smatch detected this potential error pointer dereference clk_wzrd_register_divider(). If devm_clk_hw_register() fails then it sets "hw" to an error pointer and then dereferences it on the next line. Return the error directly instead.	N/A	More Details
CVE-2023-53808	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: fix memory leak in mwifiex_histogram_read() Always free the zeroed page on return from 'mwifiex_histogram_read()'.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: l2tp: Avoid possible recursive deadlock in l2tp_tunnel_register() When a		

CVE-2023-53809	file descriptor of pppol2tp socket is passed as file descriptor of UDP socket, a recursive deadlock occurs in l2tp_tunnel_register(). This situation is reproduced by the following program: int main(void) { int sock; struct sockaddr_pppol2tp addr; sock = socket(AF_PPPOX, SOCK_DGRAM, PX_PROTO_OL2TP); if (sock < 0) { perror("socket"); return 1; } addr.sa_family = AF_PPPOX; addr.sa_protocol = PX_PROTO_OL2TP; addr.pppol2tp.pid = 0; addr.pppol2tp.fd = sock; addr.pppol2tp.addr.sin_family = PF_INET; addr.pppol2tp.addr.sin_port = htons(0); addr.pppol2tp.addr.sin_addr.s_addr = inet_addr("192.168.0.1"); addr.pppol2tp.s_tunnel = 1; addr.pppol2tp.s_session = 0; addr.pppol2tp.d_tunnel = 0; addr.pppol2tp.d_session = 0; if (connect(sock, (const struct sockaddr *)&addr, sizeof(addr)) < 0) { perror("connect"); return 1; } return 0; } This program causes the following lockdep warning: == WARNING: possible recursive locking detected 6.2.0-rc5-00205-gc96618275234 #56 Not tainted -- repro/8607 is trying to acquire lock: ffff8880213c8130 (sk_lock-AF_PPPOX){+.+.}-{0:0}, at: l2tp_tunnel_register+0x2b7/0x11c0 but task is already holding lock: ffff8880213c8130 (sk_lock-AF_PPPOX){+.+.}-{0:0}, at: pppol2tp_connect+0xa82/0x1a30 other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(sk_lock-AF_PPPOX); lock(sk_lock-AF_PPPOX); *** DEADLOCK *** May be due to missing lock nesting notation 1 lock held by repro/8607: #0: ffff8880213c8130 (sk_lock-AF_PPPOX){+.+.}-{0:0}, at: pppol2tp_connect+0xa82/0x1a30 stack backtrace: CPU: 0 PID: 8607 Comm: repro Not tainted 6.2.0-rc5-00205-gc96618275234 #56 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x100/0x178 __lock_acquire.cold+0x119/0x3b9 ? lockdep_hardirqs_on_prepare+0x410/0x410 lock_acquire+0x1e0/0x610 ? l2tp_tunnel_register+0x2b7/0x11c0 ? lock_downgrade+0x710/0x710 ? __fget_files+0x283/0x3e0 lock_sock_nested+0x3a/0xf0 ? l2tp_tunnel_register+0x2b7/0x11c0 l2tp_tunnel_register+0x2b7/0x11c0 ? sprintf+0xc4/0x100 ? l2tp_tunnel_del_work+0x6b0/0x6b0 ? debug_object_deactivate+0x320/0x320 ? lockdep_init_map_type+0x16d/0x7a0 ? lockdep_init_map_type+0x16d/0x7a0 ? l2tp_tunnel_create+0x2bf/0x4b0 ? l2tp_tunnel_create+0x3c6/0x4b0 pppol2tp_connect+0x14e1/0x1a30 ? pppol2tp_put_sk+0xd0/0xd0 ? aa_sk_perm+0x2b7/0xa80 ? aa_af_perm+0x260/0x260 ? bpf_lsm_socket_connect+0x9/0x10 ? pppol2tp_put_sk+0xd0/0xd0 __sys_connect_file+0x14f/0x190 __sys_connect+0x133/0x160 ? __sys_connect_file+0x190/0x190 ? lockdep_hardirqs_on+0x7d/0x100 ? ktime_get_coarse_real_ts64+0x1b7/0x200 ? ktime_get_coarse_real_ts64+0x147/0x200 ? __audit_syscall_entry+0x396/0x500 __x64_sys_connect+0x72/0xb0 do_syscall_64+0x38/0xb0 entry_SYSCALL_64_after_hwframe+0x63/0xcd This patch fixes the issue by getting/creating the tunnel before locking the pppol2tp socket.	N/A	More Details
CVE-2023-53810	In the Linux kernel, the following vulnerability has been resolved: blk-mq: release crypto keyslot before reporting I/O complete Once all I/O using a blk_crypto_key has completed, filesystems can call blk_crypto_evict_key(). However, the block layer currently doesn't call blk_crypto_put_keyslot() until the request is being freed, which happens after upper layers have been told (via bio_endio()) the I/O has completed. This causes a race condition where blk_crypto_evict_key() can see 'slot_refs != 0' without there being an actual bug. This makes __blk_crypto_evict_key() hit the 'WARN_ON_ONCE(atomic_read(&slot->slot_refs) != 0)' and return without doing anything, eventually causing a use-after-free in blk_crypto_reprogram_all_keys(). (This is a very rare bug and has only been seen when per-file keys are being used with fscrypt.) There are two options to fix this: either release the keyslot before bio_endio() is called on the request's last bio, or make __blk_crypto_evict_key() ignore slot_refs. Let's go with the first solution, since it preserves the ability to report bugs (via WARN_ON_ONCE) where a key is evicted while still in-use.	N/A	More Details
CVE-2023-53811	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Cap MSIX used to online CPUs + 1 The irdma driver can use a maximum number of msix vectors equal to num_online_cpus() + 1 and the kernel warning stack below is shown if that number is exceeded. The kernel throws a warning as the driver tries to update the affinity hint with a CPU mask greater than the max CPU IDs. Fix this by capping the MSIX vectors to num_online_cpus() + 1. WARNING: CPU: 7 PID: 23655 at include/linux/cpumask.h:106 irdma_cfg_ceq_vector+0x34c/0x3f0 [irdma] RIP: 0010:irdma_cfg_ceq_vector+0x34c/0x3f0 [irdma] Call Trace: irdma_rt_init_hw+0xa62/0x1290 [irdma] ? irdma_alloc_local_mac_entry+0x1a0/0x1a0 [irdma] ? __is_kernel_percpu_address+0x63/0x310 ? rcu_read_lock_held_common+0xe/0xb0 ? irdma_lan_unregister_qset+0x280/0x280 [irdma] ? irdma_request_reset+0x80/0x80 [irdma] ? ice_get_qos_params+0x84/0x390 [ice] irdma_probe+0xa40/0xfc0 [irdma] ? rcu_read_lock_bh_held+0xd0/0xd0 ? irdma_remove+0x140/0x140 [irdma] ? rcu_read_lock_sched_held+0x62/0xe0 ? down_write+0x187/0x3d0 ? auxiliary_match_id+0xf0/0x1a0 ? irdma_remove+0x140/0x140 [irdma] auxiliary_bus_probe+0xa6/0x100 __driver_probe_device+0x4a4/0xd50 ? __device_attach_driver+0x2c0/0x2c0 driver_probe_device+0x4a/0x110 __driver_attach+0x1aa/0x350 bus_for_each_dev+0x11d/0x1b0 ? subsys_dev_iter_init+0xe0/0xe0 bus_add_driver+0x3b1/0x610 driver_register+0x18e/0x410 ? 0xffffffffc0b88000 irdma_init_module+0x50/0xaa [irdma] do_one_initcall+0x103/0x5f0 ? perf_trace_initcall_level+0x420/0x420 ? do_init_module+0x4e/0x700 ? __kasan_kmalloc+0x7d/0xa0 ? kmem_cache_alloc_trace+0x188/0x2b0 ? kasan_unpoison+0x21/0x50 do_init_module+0x1d1/0x700 load_module+0x3867/0x5260 ? layout_and_allocate+0x3990/0x3990 ? rcu_read_lock_held_common+0xe/0xb0 ? rcu_read_lock_sched_held+0x62/0xe0 ? rcu_read_lock_bh_held+0xd0/0xd0 ? __vmalloc_node_range+0x46b/0x890 ? lock_release+0x5c8/0xba0 ? alloc_vm_area+0x120/0x120 ? selinux_kernel_module_from_file+0x2a5/0x300 ? __inode_security_revalidate+0xf0/0xf0 ? __do_sys_init_module+0x1db/0x260 __do_sys_init_module+0x1db/0x260 ? load_module+0x5260/0x5260 ? do_syscall_64+0x22/0x450 do_syscall_64+0xa5/0x450 entry_SYSCALL_64_after_hwframe+0x66/0xdb	N/A	More Details
CVE-2023-53812	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: fix decoder disable pm crash Can't call pm_runtime_disable when the architecture support sub device for 'dev->pm.dev' is NUll, or will get below crash log. [10.771551] pc : _raw_spin_lock_irq+0x4c/0xa0 [10.771556] lr : __pm_runtime_disable+0x30/0x130 [10.771558] sp : ffffffc01e4cb800 [10.771559] x29: ffffffc01e4cb800 x28: ffffffdf082108a8 [10.771563] x27: ffffffc01e4cbd70 x26: ffffff8605df55f0 [10.771567] x25: 0000000000000002 x24: 0000000000000002 [10.771570] x23: ffffff85c0dc9c00 x22: 0000000000000001 [10.771573] x21: 0000000000000001 x20: 0000000000000000 [10.771577] x19: 00000000000000f4 x18: ffffffdf2e9fbe18 [10.771580] x17: 0000000000000000 x16: ffffffdf2df13c74 [10.771583] x15: 00000000000002ea x14: 0000000000000058 [10.771587] x13: ffffffdf2de1b62c x12: ffffffdf2e9e30e4 [10.771590] x11: 0000000000000000 x10: 0000000000000001 [10.771593] x9 : 0000000000000000 x8 : 00000000000000f4 [10.771596] x7 : 6bff6264632c6264 x6 : 0000000000008000 [10.771600] x5 : 0080000000000000 x4 : 0000000000000001 [10.771603] x3 : 0000000000000008 x2 : 0000000000000001 [10.771608] x1 : 0000000000000000 x0 : 00000000000000f4 [10.771613] Call trace: [10.771617] _raw_spin_lock_irq+0x4c/0xa0 [10.771620] __pm_runtime_disable+0x30/0x130 [10.771657] mtk_vcodec_probe+0x69c/0x728 [mtk_vcodec_dec 800cc929d6631f79f9b273254c8db94d0d3500dc] [10.771662] platform_drv_probe+0x9c/0xbc [10.771665] really_probe+0x13c/0x3a0 [10.771668] driver_probe_device+0x84/0xc0 [10.771671] device_driver_attach+0x54/0x78	N/A	More Details
CVE-2023-53813	In the Linux kernel, the following vulnerability has been resolved: ext4: fix rbtree traversal bug in ext4_mb_use_preallocated During allocations, while looking for preallocations(PA) in the per inode rbtree, we can't do a direct traversal of the tree because ext4_mb_discard_group_preallocation() can paralelly mark the pa deleted and that can cause direct traversal to skip some entries. This was leading to a BUG_ON() being hit [1] when we missed a PA that could satisfy our request and ultimately tried to create a new PA that would overlap with the missed one. To makes sure we handle that case while still keeping the performance of the rbtree, we make use of the fact that the only pa that could possibly overlap the original goal start is the one that satisfies the below conditions: 1. It must have it's logical start immediately to the left of (ie less than) original logical start. 2. It must not be deleted To find this pa we use the following traversal method: 1. Descend into the rbtree normally to find the immediate neighboring PA. Here we keep descending irrespective of if the PA is deleted or if it overlaps with our request etc. The goal is to find an immediately adjacent PA. 2. If the found PA is on right of original goal, use rb_prev() to find the left adjacent PA. 3. Check if this PA is deleted and keep moving left with rb_prev() until a non deleted PA is found. 4. This is the PA we are looking for. Now we can check if it can satisfy the original request and proceed accordingly. This approach also takes care of having deleted PAs in the tree. (While we are at it, also fix a possible overflow bug in calculating the end	N/A	More Details

	of a PA) [1] https://lore.kernel.org/linux-ext4/CA+G9fYv2FRpLqBZf34ZinR8bU2_ZRAUOjKAD3+tKRFaEQHtt8Q@mail.gmail.com/		
CVE-2023-53814	In the Linux kernel, the following vulnerability has been resolved: PCI: Fix dropping valid root bus resources with .end = zero On r8a7791/koelsch: kmemleak: 1 new suspected memory leaks (see /sys/kernel/debug/kmemleak) # cat /sys/kernel/debug/kmemleak unreferenced object 0xc3a34e00 (size 64): comm "swapper/0", pid 1, jiffies 4294937460 (age 199.080s) hex dump (first 32 bytes): b4 5d 81 f0 b4 5d 81 f0 c0 b0 a2 c3 00 00 00 00 .]...]..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<fe3aa979>] __kmalloc+0xf0/0x140 [<34bd6bc0>] resource_list_create_entry+0x18/0x38 [<767046bc>] pci_add_resource_offset+0x20/0x68 [<b3f3edf2>] devm_of_pci_get_host_bridge_resources.constprop.0+0xb0/0x390 When coalescing two resources for a contiguous aperture, the second resource is enlarged to cover the full contiguous range, while the first resource is marked invalid. This invalidation is done by clearing the flags, start, and end members. When adding the initial resources to the bus later, invalid resources are skipped. Unfortunately, the check for an invalid resource considers only the end member, causing false positives. E.g. on r8a7791/koelsch, root bus resource 0 ("bus 00") is skipped, and no longer registered with pci_bus_insert_busn_res() (causing the memory leak), nor printed: pci-rcar-gen2 ee090000.pci: host bridge /soc/pci@ee090000 ranges: pci-rcar-gen2 ee090000.pci: MEM 0x00ee080000..0x00ee08ffff -> 0x00ee080000 pci-rcar-gen2 ee090000.pci: PCI: revision 11 pci-rcar-gen2 ee090000.pci: PCI host bridge to bus 0000:00 -pci_bus 0000:00: root bus resource [bus 00] pci_bus 0000:00: root bus resource [mem 0xee080000-0xee08ffff] Fix this by only skipping resources where all of the flags, start, and end members are zero.	N/A	More Details
CVE-2023-53815	In the Linux kernel, the following vulnerability has been resolved: posix-timers: Prevent RT livelock in itimer_delete() itimer_delete() has a retry loop when the timer is concurrently expired. On non-RT kernels this just spin-waits until the timer callback has completed, except for posix CPU timers which have HAVE_POSIX_CPU_TIMERS_TASK_WORK enabled. In that case and on RT kernels the existing task could live lock when preempting the task which does the timer delivery. Replace spin_unlock() with an invocation of timer_wait_running() to handle it the same way as the other retry loops in the posix timer code.	N/A	More Details
CVE-2023-53816	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: fix potential kgd_mem UAFs kgd_mem pointers returned by kfd_process_device_translate_handle are only guaranteed to be valid while p->mutex is held. As soon as the mutex is unlocked, another thread can free the BO.	N/A	More Details
CVE-2023-53817	In the Linux kernel, the following vulnerability has been resolved: crypto: lib/mpi - avoid null pointer deref in mpi_cmp_ui() During NVMeTCP Authentication a controller can trigger a kernel oops by specifying the 8192 bit Diffie Hellman group and passing a correctly sized, but zeroed Diffie Hellamn value. mpi_cmp_ui() was detecting this if the second parameter was 0, but 1 is passed from dh_is_pubkey_valid(). This causes the null pointer u->d to be dereferenced towards the end of mpi_cmp_ui()	N/A	More Details
CVE-2023-53818	In the Linux kernel, the following vulnerability has been resolved: ARM: zynq: Fix refcount leak in zynq_early_slcr_init of_find_compatible_node() returns a node pointer with refcount incremented, we should use of_node_put() on error path. Add missing of_node_put() to avoid refcount leak.	N/A	More Details
CVE-2023-53819	In the Linux kernel, the following vulnerability has been resolved: amdgpu: validate offset_in_bo of drm_amdgpu_gem_va This is motivated by OOB access in amdgpu_vm_update_range when offset_in_bo+map_size overflows. v2: keep the validations in amdgpu_vm_bo_map v3: add the validations to amdgpu_vm_bo_map/amdgpu_vm_bo_replace_map rather than to amdgpu_gem_va_ioctl	N/A	More Details
CVE-2025-13938	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS (Autotask Technology Integration module) allows Stored XSS.This issue affects Fireware OS 12.4 up to and including 12.11.4, 12.5 up to and including 12.5.13, and 2025.1 up to and including 2025.1.2.	N/A	More Details
CVE-2025-66490	Traefik is an HTTP reverse proxy and load balancer. For versions prior to 2.11.32 and 2.11.31 through 3.6.2, requests using PathPrefix, Path or PathRegex matchers can bypass path normalization. When Traefik uses path-based routing, requests containing URL-encoded restricted characters (/, \, Null, ;, ?, #) can bypass the middleware chain and reach unintended backends. For example, a request to http://mydomain.example.com/admin%2F could reach service-a without triggering my-security-middleware, bypassing security controls for the /admin/ path. This issue is fixed in versions 2.11.32 and 3.6.3.	N/A	More Details
CVE-2022-50657	In the Linux kernel, the following vulnerability has been resolved: riscv: mm: add missing memcpy in kasan_init Hi Atish, It seems that the panic is due to the missing memcpy during kasan_init. Could you please check whether this patch is helpful? When doing kasan_populate, the new allocated base_pud/base_p4d should contain kasan_early_shadow_{pud, p4d}'s content. Add the missing memcpy to avoid page fault when read/write kasan shadow region. Tested on: - qemu with sv57 and CONFIG_KASAN on. - qemu with sv48 and CONFIG_KASAN on.	N/A	More Details
CVE-2022-50658	In the Linux kernel, the following vulnerability has been resolved: cpufreq: qcom: fix memory leak in error path If for some reason the speedbin length is incorrect, then there is a memory leak in the error path because we never free the speedbin buffer. This commit fixes the error path to always free the speedbin buffer.	N/A	More Details
CVE-2022-50659	In the Linux kernel, the following vulnerability has been resolved: hwrng: geode - Fix PCI device refcount leak for_each_pci_dev() is implemented by pci_get_device(). The comment of pci_get_device() says that it will increase the reference count for the returned pci_dev and also decrease the reference count for the input pci_dev @from if it is not NULL. If we break for_each_pci_dev() loop with pdev not NULL, we need to call pci_dev_put() to decrease the reference count. We add a new struct 'amd_geode_priv' to record pointer of the pci_dev and membase, and then add missing pci_dev_put() for the normal and error path.	N/A	More Details
CVE-2022-50660	In the Linux kernel, the following vulnerability has been resolved: wifi: ipw2200: fix memory leak in ipw_wdev_init() In the error path of ipw_wdev_init(), exception value is returned, and the memory applied for in the function is not released. Also the memory is not released in ipw_pci_probe(). As a result, memory leakage occurs. So memory release needs to be added to the error path of ipw_wdev_init().	N/A	More Details
CVE-2023-53804	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix use-after-free bug of nilfs_root in nilfs_evict_inode() During unmount process of nilfs2, nothing holds nilfs_root structure after nilfs2 detaches its writer in nilfs_detach_log_writer(). However, since nilfs_evict_inode() uses nilfs_root for some cleanup operations, it may cause use-after-free read if inodes are left in "garbage_list" and released by nilfs_dispose_list() at the end of nilfs_detach_log_writer(). Fix this issue by modifying nilfs_evict_inode() to only clear inode without additional metadata changes that use nilfs_root if the file system is degraded to read-only or the writer is detached.	N/A	More Details
CVE-2023-53803	In the Linux kernel, the following vulnerability has been resolved: scsi: ses: Fix slab-out-of-bounds in ses_enclosure_data_process() A fix for: BUG: KASAN: slab-out-of-bounds in ses_enclosure_data_process+0x949/0xe30 [ses] Read of size 1 at addr ffff88a1b043a451 by task systemd-udevd/3271 Checking after (and before in next loop) addl_desc_ptr[1] is sufficient, we expect the size to be sanitized before first access to addl_desc_ptr[1]. Make sure we don't walk beyond end of page.	N/A	More Details
CVE-2023-53802	In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: htc_hst: free skb in ath9k_htc_rx_msg() if there is no callback function It is stated that ath9k_htc_rx_msg() either frees the provided skb or passes its management to another callback function. However, the skb is not freed in case there is no another callback function, and Syzkaller was able to cause a memory leak. Also minor comment fix. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: bpf: Zeroing allocated object from slab in bpf memory allocator Currently the freed element in bpf memory allocator may be immediately reused, for htab map the reuse will reinitialize special fields in map value		

CVE-2023-53790	(e.g., bpf_spin_lock), but lookup procedure may still access these special fields, and it may lead to hard-lockup as shown below: NMI backtrace for cpu 16 CPU: 16 PID: 2574 Comm: htab.bin Tainted: G L 6.1.0+ #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), RIP: 0010:queued_spin_lock_slowpath+0x283/0x2c0 ..... Call Trace: <TASK> copy_map_value_locked+0xb7/0x170 bpf_map_copy_value+0x113/0x3c0 __sys_bpf+0x1c67/0x2780 __x64_sys_bpf+0x1c/0x20 do_syscall_64+0x30/0x60 entry_SYSCALL_64_after_hwframe+0x46/0xb0 ..... </TASK> For htab map, just like the preallocated case, these is no need to initialize these special fields in map value again once these fields have been initialized. For preallocated htab map, these fields are initialized through __GFP_ZERO in bpf_map_area_alloc(), so do the similar thing for non-preallocated htab in bpf memory allocator. And there is no need to use __GFP_ZERO for per-cpu bpf memory allocator, because __alloc_percpu_gfp() does it implicitly.	N/A	More Details
CVE-2023-53781	In the Linux kernel, the following vulnerability has been resolved: smc: Fix use-after-free in tcp_write_timer_handler(). With Eric's ref tracker, syzbot finally found a repro for use-after-free in tcp_write_timer_handler() by kernel TCP sockets. [0] If SMC creates a kernel socket in __smc_create(), the kernel socket is supposed to be freed in smc_clcsock_release() by calling sock_release() when we close() the parent SMC socket. However, at the end of smc_clcsock_release(), the kernel socket's sk_state might not be TCP_CLOSE. This means that we have not called inet_csk_destroy_sock() in __tcp_close() and have not stopped the TCP timers. The kernel socket's TCP timers can be fired later, so we need to hold a refcnt for net as we do for MPTCP subflows in mptcp_subflow_create_socket(). [0]: leaked reference. sk_alloc (./include/net/net_namespace.h:335 net/core/sock.c:2108) inet_create (net/ipv4/af_inet.c:319 net/ipv4/af_inet.c:244) __sock_create (net/socket.c:1546) smc_create (net/smc/af_smc.c:3269 net/smc/af_smc.c:3284) __sock_create (net/socket.c:1546) __sys_socket (net/socket.c:1634 net/socket.c:1618 net/socket.c:1661) __x64_sys_socket (net/socket.c:1672) 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) == BUG: KASAN: slab-use-after-free in tcp_write_timer_handler (net/ipv4/tcp_timer.c:378 net/ipv4/tcp_timer.c:624 net/ipv4/tcp_timer.c:594) Read of size 1 at addr ffff888052b65e0d by task syzrepro/18091 CPU: 0 PID: 18091 Comm: syzrepro Tainted: G W 6.3.0-rc4-01174-gb5d54eb5899a #7 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.0-1.amzn2022.0.1 04/01/2014 Call Trace: <IRQ> dump_stack_lvl (lib/dump_stack.c:107) print_report (mm/kasan/report.c:320 mm/kasan/report.c:430) kasan_report (mm/kasan/report.c:538) tcp_write_timer_handler (net/ipv4/tcp_timer.c:378 net/ipv4/tcp_timer.c:624 net/ipv4/tcp_timer.c:594) tcp_write_timer (./include/linux/spinlock.h:390 net/ipv4/tcp_timer.c:643) call_timer_fn (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:207 ./include/trace/events/timer.h:127 kernel/time/timer.c:1701) __run_timers.part.0 (kernel/time/timer.c:1752 kernel/time/timer.c:2022) run_timer_softirq (kernel/time/timer.c:2037) __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:572) __irq_exit_rcu (kernel/softirq.c:445 kernel/softirq.c:650) irq_exit_rcu (kernel/softirq.c:664) sysvec_apic_timer_interrupt (arch/x86/kernel/apic/apic.c:1107 (discriminator 14)) </IRQ>	N/A	More Details
CVE-2023-53782	In the Linux kernel, the following vulnerability has been resolved: dccp: Fix out of bounds access in DCCP error handler There was a previous attempt to fix an out-of-bounds access in the DCCP error handlers, but that fix assumed that the error handlers only want to access the first 8 bytes of the DCCP header. Actually, they also look at the DCCP sequence number, which is stored beyond 8 bytes, so an explicit pskb_may_pull() is required.	N/A	More Details
CVE-2023-53783	In the Linux kernel, the following vulnerability has been resolved: blk-iocost: fix divide by 0 error in calc_lcoefs() echo max of u64 to cost.model can cause divide by 0 error. # echo 8:0 rbps=18446744073709551615 > /sys/fs/cgroup/io.cost.model divide error: 0000 [#1] PREEMPT SMP RIP: 0010:calc_lcoefs+0x4c/0xc0 Call Trace: <TASK> ioc_refresh_params+0x2b3/0x4f0 ioc_cost_model_write+0x3cb/0x4c0 ? _copy_from_iter+0x6d/0x6c0 ? kernfs_fop_write_iter+0xfc/0x270 cgroup_file_write+0xa0/0x200 kernfs_fop_write_iter+0x17d/0x270 vfs_write+0x414/0x620 ksys_write+0x73/0x160 __x64_sys_write+0x1e/0x30 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd calc_lcoefs() uses the input value of cost.model in DIV_ROUND_UP_ULL, overflow would happen if bps plus IOC_PAGE_SIZE is greater than ULLONG_MAX, it can cause divide by 0 error. Fix the problem by setting basecost	N/A	More Details
CVE-2023-53784	In the Linux kernel, the following vulnerability has been resolved: drm: bridge: dw_hdmi: fix connector access for scdc Commit 5d844091f237 ("drm/scdc-helper: Pimp SCDC debugs") changed the scdc interface to pick up an i2c adapter from a connector instead. However, in the case of dw-hdmi, the wrong connector was being used to pass i2c adapter information, since dw-hdmi's embedded connector structure is only populated when the bridge attachment callback explicitly asks for it. drm-meson is handling connector creation, so this won't happen, leading to a NULL pointer dereference. Fix it by having scdc functions access dw-hdmi's current connector pointer instead, which is assigned during the bridge enablement stage. [narmstrong: moved Fixes tag before first S-o-b and added Reported-by tag]	N/A	More Details
CVE-2023-53785	In the Linux kernel, the following vulnerability has been resolved: mt76: mt7921: don't assume adequate headroom for SDIO headers mt7921_usb_sdio_tx_prepare_skb() calls mt7921_usb_sdio_write_txwi() and mt7921_skb_add_usb_sdio_hdr(), both of which blindly assume that adequate headroom will be available in the passed skb. This assumption typically is satisfied when the skb was allocated in the net core for transmission via the mt7921 netdev (although even that is only an optimization and is not strictly guaranteed), but the assumption is sometimes not satisfied when the skb originated in the receive path of another netdev and was passed through to the mt7921, such as by the bridge layer. Blindly prepending bytes to an skb is always wrong. This commit introduces a call to skb_cow_head() before the call to mt7921_usb_sdio_write_txwi() in mt7921_usb_sdio_tx_prepare_skb() to ensure that at least MT_SDIO_TXD_SIZE + MT_SDIO_HDR_SIZE bytes can be pushed onto the skb. Without this fix, I can trivially cause kernel panics by bridging an MT7921AU-based USB 802.11ax interface with an Ethernet interface on an Intel Atom-based x86 system using its onboard RTL8169 PCI Ethernet adapter and also on an ARM-based Raspberry Pi 1 using its onboard SMSC9512 USB Ethernet adapter. Note that the panics do not occur in every system configuration, as they occur only if the receiving netdev leaves less headroom in its received skbs than the mt7921 needs for its SDIO headers. Here is an example stack trace of this panic on Raspberry Pi OS Lite 2023-02-21 running kernel 6.1.24+ [1]: skb_panic from skb_push+0x44/0x48 skb_push from mt7921_usb_sdio_tx_prepare_skb+0xd4/0x190 [mt7921_common] mt7921_usb_sdio_tx_prepare_skb [mt7921_common] from mt76u_tx_queue_skb+0x94/0x1d0 [mt76_usb] mt76u_tx_queue_skb [mt76_usb] from __mt76_tx_queue_skb+0x4c/0xc8 [mt76] __mt76_tx_queue_skb [mt76] from mt76_txq_schedule.part.0+0x13c/0x398 [mt76] mt76_txq_schedule.part.0 [mt76] from mt76_txq_schedule_all+0x24/0x30 [mt76] mt76_txq_schedule_all [mt76] from mt7921_tx_worker+0x58/0xf4 [mt7921_common] mt7921_tx_worker [mt7921_common] from __mt76_worker_fn+0x9c/0xec [mt76] __mt76_worker_fn [mt76] from kthread+0xbc/0xe0 kthread from ret_from_fork+0x14/0x34 After this fix, bridging the mt7921 interface works fine on both of my previously problematic systems. [1] https://github.com/raspberrypi/firmware/tree/5c276f55a4b21345cd4d6200a504ee991851ff7a	N/A	More Details
CVE-2023-53786	In the Linux kernel, the following vulnerability has been resolved: dm flakey: fix a crash with invalid table line This command will crash with NULL pointer dereference: dmsetup create flakey --table \ "0 `blockdev --getsize /dev/ram0` flakey /dev/ram0 0 0 1 2 corrupt_bio_byte 512" Fix the crash by checking if arg_name is non-NULL before comparing it.	N/A	More Details
CVE-2023-53787	In the Linux kernel, the following vulnerability has been resolved: regulator: da9063: fix null pointer deref with partial DT config When some of the da9063 regulators do not have corresponding DT nodes a null pointer dereference occurs on boot because such regulators have no init_data causing the pointers calculated in da9063_check_xvp_constraints() to be invalid. Do not dereference them in this case.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda/ca0132: fixup buffer overrun at tuning_ctl_set() tuning_ctl_set() might have buffer overrun at (X) if it didn't break from loop by matching (A). static int tuning_ctl_set(...) { for (i = 0; i < TUNING_CTLS_COUNT; i++) (A) if (nid == ca0132_tuning_ctls[i].nid) break; snd_hda_power_up(...); (X) dspio_set_param(...,		More

2023-53788	ca0132_tuning_ctls[i].mid, ...); snd_hda_power_down(...); ^ return 1; } We will get below error by cppcheck sound/pci/hda/patch_ca0132.c:4229:2: note: After for loop, i has value 12 for (i = 0; i < TUNING_CTLS_COUNT; i++) ^ sound/pci/hda/patch_ca0132.c:4234:43: note: Array index out of bounds dspio_set_param(codec, ca0132_tuning_ctls[i].mid, 0x20, ^ This patch cares non match case.	N/A	Details
CVE-2023-53789	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Improve page fault error reporting If IOMMU domain for device group is not setup properly then we may hit IOMMU page fault. Current page fault handler assumes that domain is always setup and it will hit NULL pointer derefence (see below sample log). Lets check whether domain is setup or not and log appropriate message. Sample log: ---------- amdgpu 0000:00:01.0: amdgpu: SE 1, SH per SE 1, CU per SH 8, active_cu_number 6 BUG: kernel NULL pointer dereference, address: 0000000000000058 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 2 PID: 56 Comm: irq/24-AMD-Vi Not tainted 6.2.0-rc2+ #89 Hardware name: xxx RIP: 0010:report_iommu_fault+0x11/0x90 [...] Call Trace: <TASK> amd_iommu_int_thread+0x60c/0x760 ? __pfx_irq_thread_fn+0x10/0x10 irq_thread_fn+0x1f/0x60 irq_thread+0xea/0x1a0 ? preempt_count_add+0x6a/0xa0 ? __pfx_irq_thread_dtor+0x10/0x10 ? __pfx_irq_thread+0x10/0x10 kthread+0xe9/0x110 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2c/0x50 </TASK> [joro: Edit commit message]	N/A	More Details
CVE-2023-53791	In the Linux kernel, the following vulnerability has been resolved: md: fix warning for holder mismatch from export_rdev() Commit a1d767191096 ("md: use mddev->external to select holder in export_rdev()") fix the problem that 'claim_rdev' is used for blkdev_get_by_dev() while 'rdev' is used for blkdev_put(). However, if mddev->external is changed from 0 to 1, then 'rdev' is used for blkdev_get_by_dev() while 'claim_rdev' is used for blkdev_put(). And this problem can be reporduced reliably by following: New file: mdadm/tests/23rdev-lifetime devname=${dev0##*/} devt=`cat /sys/block/$devname/dev` pid="" runtime=2 clean_up_test() { pill -9 $pid echo clear > /sys/block/md0/md/array_state } trap 'clean_up_test' EXIT add_by_sysfs() { while true; do echo $devt > /sys/block/md0/md/new_dev done } remove_by_sysfs(){ while true; do echo remove > /sys/block/md0/md/dev-${devname}/state done } echo md0 > /sys/module/md_mod/parameters/new_array || die "create md0 failed" add_by_sysfs & pid="$pid $!" remove_by_sysfs & pid="$pid $!" sleep $runtime exit 0 Test cmd: ./test --save-logs --logdir=/tmp/ --keep-going --dev=loop --tests=23rdev-lifetime Test result: ------------[cut here]------------ WARNING: CPU: 0 PID: 960 at block/bdev.c:618 blkdev_put+0x27c/0x330 Modules linked in: multipath md_mod loop CPU: 0 PID: 960 Comm: test Not tainted 6.5.0-rc2-00121-g01e55c376936-dirty #50 RIP: 0010:blkdev_put+0x27c/0x330 Call Trace: <TASK> export_rdev.isra.23+0x50/0xa0 [md_mod] mddev_unlock+0x19d/0x300 [md_mod] rdev_attr_store+0xec/0x190 [md_mod] sysfs_kf_write+0x52/0x70 kernfs_fop_write_iter+0x19a/0x2a0 vfs_write+0x3b5/0x770 ksys_write+0x74/0x150 __x64_sys_write+0x22/0x30 do_syscall_64+0x40/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd Fix the problem by recording if 'rdev' is used as holder.	N/A	More Details
CVE-2023-53801	In the Linux kernel, the following vulnerability has been resolved: iommu/sprd: Release dma buffer to avoid memory leak When attaching to a domain, the driver would alloc a DMA buffer which is used to store address mapping table, and it need to be released when the IOMMU domain is freed.	N/A	More Details
CVE-2023-53792	In the Linux kernel, the following vulnerability has been resolved: nvme-core: fix memory leak in dhchap_ctrl_secret Free dhchap_secret in nvme_ctrl_dhchap_ctrl_secret_store() before we return when nvme_auth_generate_key() returns error.	N/A	More Details
CVE-2023-53793	In the Linux kernel, the following vulnerability has been resolved: perf tool x86: Fix perf_env memory leak Found by leak sanitizer: ``` ==1632594==ERROR: LeakSanitizer: detected memory leaks Direct leak of 21 byte(s) in 1 object(s) allocated from: #0 0x7f2953a7077b in __interceptor_strdup ../../../../src/libsanitizer/asan/asan_interceptors.cpp:439 #1 0x556701d6fbbf in perf_env__read_cpuid util/env.c:369 #2 0x556701d70589 in perf_env__cpuid util/env.c:465 #3 0x55670204bba2 in x86__is_amd_cpu arch/x86/util/env.c:14 #4 0x5567020487a2 in arch__post_evsel_config arch/x86/util/evsel.c:83 #5 0x556701d8f78b in evsel__config util/evsel.c:1366 #6 0x556701ef5872 in evlist__config util/record.c:108 #7 0x556701cd6bcd in test__PERF_RECORD tests/perf-record.c:112 #8 0x556701cacd07 in run_test tests/builtin-test.c:236 #9 0x556701cacfac in test_and_print tests/builtin-test.c:265 #10 0x556701cadddb in __cmd_test tests/builtin-test.c:402 #11 0x556701caf2aa in cmd_test tests/builtin-test.c:559 #12 0x556701d3b557 in run_builtin tools/perf/perf.c:323 #13 0x556701d3bac8 in handle_internal_command tools/perf/perf.c:377 #14 0x556701d3be90 in run_argv tools/perf/perf.c:421 #15 0x556701d3c3f8 in main tools/perf/perf.c:537 #16 0x7f2952a46189 in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58 SUMMARY: AddressSanitizer: 21 byte(s) leaked in 1 allocation(s). ```	N/A	More Details
CVE-2023-53794	In the Linux kernel, the following vulnerability has been resolved: cifs: fix session state check in reconnect to avoid use-after-free issue Don't collect exiting session in smb2_reconnect_server(), because it will be released soon. Note that the exiting session will stay in server->smb_ses_list until it complete the cifs_free_ipc() and logoff() and then delete itself from the list.	N/A	More Details
CVE-2023-53795	In the Linux kernel, the following vulnerability has been resolved: iommufd: IOMMUFD_DESTROY should not increase the refcount syzkaller found a race where IOMMUFD_DESTROY increments the refcount: obj = iommufd_get_object(ucmd->ictx, cmd->id, IOMMUFD_OBJ_ANY); if (IS_ERR(obj)) return PTR_ERR(obj); iommufd_ref_to_users(obj); /* See iommufd_ref_to_users() */ if (!iommufd_object_destroy_user(ucmd->ictx, obj)) As part of the sequence to join the two existing primitives together. Allowing the refcount the be elevated without holding the destroy_rwsem violates the assumption that all temporary refcount elevations are protected by destroy_rwsem. Racing IOMMUFD_DESTROY with iommufd_object_destroy_user() will cause spurious failures: WARNING: CPU: 0 PID: 3076 at drivers/iommu/iommufd/device.c:477 iommufd_access_destroy+0x18/0x20 drivers/iommu/iommufd/device.c:478 Modules linked in: CPU: 0 PID: 3076 Comm: syz-executor.0 Not tainted 6.3.0-rc1-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/03/2023 RIP: 0010:iommufd_access_destroy+0x18/0x20 drivers/iommu/iommufd/device.c:477 Code: e8 3d 4e 00 00 84 c0 74 01 c3 0f 0b c3 0f 1f 44 00 00 f3 0f 1e fa 48 89 fe 48 8b bf a8 00 00 00 e8 1d 4e 00 00 84 c0 74 01 c3 <0f> 0b c3 0f 1f 44 00 00 41 57 41 56 41 55 4c 8d ae d0 00 00 00 41 RSP: 0018:ffffc90003067e08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff888109ea0300 RCX: 0000000000000000 RDX: 0000000000000001 RSI: 0000000000000000 RDI: 00000000ffffffff RBP: 0000000000000004 R08: 0000000000000000 R09: ffff88810bbb3500 R10: ffff88810bbb3e48 R11: 0000000000000000 R12: ffffc90003067e88 R13: ffffc90003067ea8 R14: ffff888101249800 R15: 00000000fffffffe FS: 00007ff7254fe6c0(0000) GS:ffff888237c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000555557262da8 CR3: 000000010a6fd000 CR4: 0000000000350ef0 Call Trace: <TASK> iommufd_test_create_access drivers/iommu/iommufd/selftest.c:596 [inline] iommufd_test+0x71c/0xcf0 drivers/iommu/iommufd/selftest.c:813 iommufd_fops_ioctl+0x10f/0x1b0 drivers/iommu/iommufd/main.c:337 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:870 [inline] __se_sys_ioctl fs/ioctl.c:856 [inline] __x64_sys_ioctl+0x84/0xc0 fs/ioctl.c:856 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x38/0x80 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd The solution is to not increment the refcount on the IOMMUFD_DESTROY path at all. Instead use the xa_lock to serialize everything. The refcount check == 1 and xa_erase can be done under a single critical region. This avoids the need for any refcount incrementing. It has the downside that if userspace races destroy with other operations it will get an EBUSY instead of waiting, but this is kind of racing is already dangerous.	N/A	More Details
CVE-2023-53796	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix information leak in f2fs_move_inline_dirents() When converting an inline directory to a regular one, f2fs is leaking uninitialized memory to disk because it doesn't initialize the entire directory block. Fix this by zero-initializing the block. This bug was introduced by commit 4ec17d688d74 ("f2fs: avoid unneeded initializing when converting inline dentry"), which didn't consider the security implications of leaking uninitialized memory to disk. This was found by running xfstest generic/435 on a KMSAN-enabled kernel.	N/A	More Details

CVE-2023-53797	In the Linux kernel, the following vulnerability has been resolved: HID: wacom: Use ktime_t rather than int when dealing with timestamps Code which interacts with timestamps needs to use the ktime_t type returned by functions like ktime_get. The int type does not offer enough space to store these values, and attempting to use it is a recipe for problems. In this particular case, overflows would occur when calculating/storing timestamps leading to incorrect values being reported to userspace. In some cases these bad timestamps cause input handling in userspace to appear hung.	N/A	More Details
CVE-2023-53798	In the Linux kernel, the following vulnerability has been resolved: ethtool: Fix uninitialized number of lanes It is not possible to set the number of lanes when setting link modes using the legacy IOCTL ethtool interface. Since 'struct ethtool_link_ksettings' is not initialized in this path, drivers receive an uninitialized number of lanes in 'struct ethtool_link_ksettings::lanes'. When this information is later queried from drivers, it results in the ethtool code making decisions based on uninitialized memory, leading to the following KMSAN splat [1]. In practice, this most likely only happens with the tun driver that simply returns whatever it got in the set operation. As far as I can tell, this uninitialized memory is not leaked to user space thanks to the 'ethtool_ops->cap_link_lanes_supported' check in linkmodes_prepare_data(). Fix by initializing the structure in the IOCTL path. Did not find any more call sites that pass an uninitialized structure when calling 'ethtool_ops::set_link_ksettings()'. [1] BUG: KMSAN: uninit-value in ethnl_update_linkmodes net/ethtool/linkmodes.c:273 [inline] BUG: KMSAN: uninit-value in ethnl_set_linkmodes+0x190b/0x19d0 net/ethtool/linkmodes.c:333 ethnl_update_linkmodes net/ethtool/linkmodes.c:273 [inline] ethnl_set_linkmodes+0x190b/0x19d0 net/ethtool/linkmodes.c:333 ethnl_default_set_doit+0x88d/0xde0 net/ethtool/netlink.c:640 genl_family_rcv_msg_doit net/netlink/genetlink.c:968 [inline] genl_family_rcv_msg net/netlink/genetlink.c:1048 [inline] genl_rcv_msg+0x141a/0x14c0 net/netlink/genetlink.c:1065 netlink_rcv_skb+0x3f8/0x750 net/netlink/af_netlink.c:2577 genl_rcv+0x40/0x60 net/netlink/genetlink.c:1076 netlink_unicast_kernel net/netlink/af_netlink.c:1339 [inline] netlink_unicast+0xf41/0x1270 net/netlink/af_netlink.c:1365 netlink_sendmsg+0x127d/0x1430 net/netlink/af_netlink.c:1942 sock_sendmsg_nosec net/socket.c:724 [inline] sock_sendmsg net/socket.c:747 [inline] ____sys_sendmsg+0xa24/0xe40 net/socket.c:2501 ___sys_sendmsg+0x2a1/0x3f0 net/socket.c:2555 __sys_sendmsg net/socket.c:2584 [inline] __do_sys_sendmsg net/socket.c:2593 [inline] __se_sys_sendmsg net/socket.c:2591 [inline] __x64_sys_sendmsg+0x36b/0x540 net/socket.c:2591 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 Uninit was stored to memory at: tun_get_link_ksettings+0x37/0x60 drivers/net/tun.c:3544 __ethtool_get_link_ksettings+0x17b/0x260 net/ethtool/ioctl.c:441 ethnl_set_linkmodes+0xee/0x19d0 net/ethtool/linkmodes.c:327 ethnl_default_set_doit+0x88d/0xde0 net/ethtool/netlink.c:640 genl_family_rcv_msg_doit net/netlink/genetlink.c:968 [inline] genl_family_rcv_msg net/netlink/genetlink.c:1048 [inline] genl_rcv_msg+0x141a/0x14c0 net/netlink/genetlink.c:1065 netlink_rcv_skb+0x3f8/0x750 net/netlink/af_netlink.c:2577 genl_rcv+0x40/0x60 net/netlink/genetlink.c:1076 netlink_unicast_kernel net/netlink/af_netlink.c:1339 [inline] netlink_unicast+0xf41/0x1270 net/netlink/af_netlink.c:1365 netlink_sendmsg+0x127d/0x1430 net/netlink/af_netlink.c:1942 sock_sendmsg_nosec net/socket.c:724 [inline] sock_sendmsg net/socket.c:747 [inline] ____sys_sendmsg+0xa24/0xe40 net/socket.c:2501 ___sys_sendmsg+0x2a1/0x3f0 net/socket.c:2555 __sys_sendmsg net/socket.c:2584 [inline] __do_sys_sendmsg net/socket.c:2593 [inline] __se_sys_sendmsg net/socket.c:2591 [inline] __x64_sys_sendmsg+0x36b/0x540 net/socket.c:2591 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 Uninit was stored to memory at: tun_set_link_ksettings+0x37/0x60 drivers/net/tun.c:3553 ethtool_set_link_ksettings+0x600/0x690 net/ethtool/ioctl.c:609 __dev_ethtool net/ethtool/ioctl.c:3024 [inline] dev_ethtool+0x1db9/0x2a70 net/ethtool/ioctl.c:3078 dev_ioctl+0xb07/0x1270 net/core/dev_ioctl.c:524 sock_do_ioctl+0x295/0x540 net/socket.c:1213 sock_i ---truncated---	N/A	More Details
CVE-2023-53799	In the Linux kernel, the following vulnerability has been resolved: crypto: api - Use work queue in crypto_destroy_instance The function crypto_drop_spawn expects to be called in process context. However, when an instance is unregistered while it still has active users, the last user may cause the instance to be freed in atomic context. Fix this by delaying the freeing to a work queue.	N/A	More Details
CVE-2023-53800	In the Linux kernel, the following vulnerability has been resolved: ubi: Fix use-after-free when volume resizing failed There is an use-after-free problem reported by KASAN: == BUG: KASAN: use-after-free in ubi_eba_copy_table+0x11f/0x1c0 [ubi] Read of size 8 at addr ffff888101eec008 by task ubirsvol/4735 CPU: 2 PID: 4735 Comm: ubirsvol Not tainted 6.1.0-rc1-00003-g84fa3304a7fc-dirty #14 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-1.fc33 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x34/0x44 print_report+0x171/0x472 kasan_report+0xad/0x130 ubi_eba_copy_table+0x11f/0x1c0 [ubi] ubi_resize_volume+0x4f9/0xbc0 [ubi] ubi_cdev_ioctl+0x701/0x1850 [ubi] __x64_sys_ioctl+0x11d/0x170 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x46/0xb0 </TASK> When ubi_change_vtbl_record() returns an error in ubi_resize_volume(), "new_eba_tbl" will be freed on error handing path, but it is holded by "vol->eba_tbl" in ubi_eba_replace_table(). It means that the liftcycle of "vol->eba_tbl" and "vol" are different, so when resizing volume in next time, it causing an use-after-free fault. Fix it by not freeing "new_eba_tbl" after it replaced in ubi_eba_replace_table(), while will be freed in next volume resizing.	N/A	More Details
CVE-2022-50661	In the Linux kernel, the following vulnerability has been resolved: seccomp: Move copy_seccomp() to no failure path. Our syzbot instance reported memory leaks in do_seccomp() [0], similar to the report [1]. It shows that we miss freeing struct seccomp_filter and some objects included in it. We can reproduce the issue with the program below [2] which calls one seccomp() and two clone() syscalls. The first clone()d child exits earlier than its parent and sends a signal to kill it during the second clone(), more precisely before the fatal_signal_pending() test in copy_process(). When the parent receives the signal, it has to destroy the embryonic process and return -EINTR to user space. In the failure path, we have to call seccomp_filter_release() to decrement the filter's refcount. Initially, we called it in free_task() called from the failure path, but the commit 3a15fb6ed92c ("seccomp: release filter after task is fully dead") moved it to release_task() to notify user space as early as possible that the filter is no longer used. To keep the change and current seccomp refcount semantics, let's move copy_seccomp() just after the signal check and add a WARN_ON_ONCE() in free_task() for future debugging. [0]: unreferenced object 0xffff8880063add00 (size 256): comm "repro_seccomp", pid 230, jiffies 4294687090 (age 9.914s) hex dump (first 32 bytes): 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 ..... ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ..... backtrace: do_seccomp (./include/linux/slab.h:600 ./include/linux/slab.h:733 kernel/seccomp.c:666 kernel/seccomp.c:708 kernel/seccomp.c:1871 kernel/seccomp.c:1991) 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) unreferenced object 0xffffc90000035000 (size 4096): comm "repro_seccomp", pid 230, jiffies 4294687090 (age 9.915s) hex dump (first 32 bytes): 01 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: __vmalloc_node_range (mm/vmalloc.c:3226) __vmalloc_node (mm/vmalloc.c:3261 (discriminator 4)) bpf_prog_alloc_no_stats (kernel/bpf/core.c:91) bpf_prog_alloc (kernel/bpf/core.c:129) bpf_prog_create_from_user (net/core/filter.c:1414) do_seccomp (kernel/seccomp.c:671 kernel/seccomp.c:708 kernel/seccomp.c:1871 kernel/seccomp.c:1991) 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) unreferenced object 0xffff888003fa1000 (size 1024): comm "repro_seccomp", pid 230, jiffies 4294687090 (age 9.915s) 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: bpf_prog_alloc_no_stats (./include/linux/slab.h:600 ./include/linux/slab.h:733 kernel/bpf/core.c:95) bpf_prog_alloc (kernel/bpf/core.c:129) bpf_prog_create_from_user (net/core/filter.c:1414) do_seccomp (kernel/seccomp.c:671 kernel/seccomp.c:708 kernel/seccomp.c:1871 kernel/seccomp.c:1991) 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) unreferenced object 0xffff888006360240 (size 16): comm "repro_seccomp", pid 230, jiffies 4294687090 (age 9.915s) hex dump (first 16 bytes): 01 00 37 00 76 65 72 6c e0 83 01 06 80 88 ff ff ..7.verl..... backtrace: bpf_prog_store_orig_filter (net/core/filter.c:1137) bpf_prog_create_from_user (net/core/filter.c:1428) do_seccomp (kernel/seccomp.c:671 kernel/seccomp.c:708 kernel/seccomp.c:1871 kernel/seccomp.c:1991) do_syscall_64 (arch/x86/entry/common.c:50	N/A	More Details

	arch/x86/entry/common.c:80) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:120) unreferenced object 0xffff888 ---truncated---		
CVE-2022-50662	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: fix memory leak in hns_roce_alloc_mr() When hns_roce_mr_enable() failed in hns_roce_alloc_mr(), mr_key is not released. Compiled test only.	N/A	More Details
CVE-2022-50663	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix possible memory leak in stmmac_dvr_probe() The bitmap_free() should be called to free priv->af_xdp_zc_qps when create_singlethread_workqueue() fails, otherwise there will be a memory leak, so we add the err path error_wq_init to fix it.	N/A	More Details
CVE-2023-53838	In the Linux kernel, the following vulnerability has been resolved: f2fs: synchronize atomic write aborts To fix a race condition between atomic write aborts, I use the inode lock and make COW inode to be re-usable thoroughout the whole atomic file inode lifetime.	N/A	More Details
CVE-2023-53829	In the Linux kernel, the following vulnerability has been resolved: f2fs: flush inode if atomic file is aborted Let's flush the inode being aborted atomic operation to avoid stale dirty inode during eviction in this call stack: f2fs_mark_inode_dirty_sync+0x22/0x40 [f2fs] f2fs_abort_atomic_write+0xc4/0xf0 [f2fs] f2fs_evict_inode+0x3f/0x690 [f2fs] ? sugov_start+0x140/0x140 evict+0xc3/0x1c0 evict_inodes+0x17b/0x210 generic_shutdown_super+0x32/0x120 kill_block_super+0x21/0x50 deactivate_locked_super+0x31/0x90 cleanup_mnt+0x100/0x160 task_work_run+0x59/0x90 do_exit+0x33b/0xa50 do_group_exit+0x2d/0x80 __x64_sys_exit_group+0x14/0x20 do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd This triggers f2fs_bug_on() in f2fs_evict_inode: f2fs_bug_on(sbi, is_inode_flag_set(inode, FI_DIRTY_INODE)); This fixes the syzbot report: loop0: detected capacity change from 0 to 131072 F2FS-fs (loop0): invalid crc value F2FS-fs (loop0): Found nat_bits in checkpoint F2FS-fs (loop0): Mounted with checkpoint version = 48b305e4 ------------[cut here]------------ kernel BUG at fs/f2fs/inode.c:869! invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 0 PID: 5014 Comm: syz-executor220 Not tainted 6.4.0-syzkaller-11479-g6cd06ab12d1a #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/27/2023 RIP: 0010:f2fs_evict_inode+0x172d/0x1e00 fs/f2fs/inode.c:869 Code: ff df 48 c1 ea 03 80 3c 02 00 0f 85 6a 06 00 00 8b 75 40 ba 01 00 00 00 4c 89 e7 e8 6d ce 06 00 e9 aa fc ff ff e8 63 22 e2 fd <0f> 0b e8 5c 22 e2 fd 48 c7 c0 a8 3a 18 8d 48 ba 00 00 00 00 00 fc RSP: 0018:ffffc90003a6fa00 EFLAGS: 00010293 RAX: 0000000000000000 RBX: 0000000000000001 RCX: 0000000000000000 RDX: ffff8880273b8000 RSI: ffffffff83a2bd0d RDI: 0000000000000007 RBP: ffff888077db91b0 R08: 0000000000000007 R09: 0000000000000000 R10: 0000000000000001 R11: 0000000000000001 R12: ffff888029a3c000 R13: ffff888077db9660 R14: ffff888029a3c0b8 R15: ffff888077db9c50 FS: 0000000000000000(0000) GS:ffff8880b9800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f1909bb9000 CR3: 00000000276a9000 CR4: 0000000000350ef0 Call Trace: <TASK> evict+0x2ed/0x6b0 fs/inode.c:665 dispose_list+0x117/0x1e0 fs/inode.c:698 evict_inodes+0x345/0x440 fs/inode.c:748 generic_shutdown_super+0xaf/0x480 fs/super.c:478 kill_block_super+0x64/0xb0 fs/super.c:1417 kill_f2fs_super+0x2af/0x3c0 fs/f2fs/super.c:4704 deactivate_locked_super+0x98/0x160 fs/super.c:330 deactivate_super+0xb1/0xd0 fs/super.c:361 cleanup_mnt+0x2ae/0x3d0 fs/namespace.c:1254 task_work_run+0x16f/0x270 kernel/task_work.c:179 exit_task_work include/linux/task_work.h:38 [inline] do_exit+0xa9a/0x29a0 kernel/exit.c:874 do_group_exit+0xd4/0x2a0 kernel/exit.c:1024 __do_sys_exit_group kernel/exit.c:1035 [inline] __se_sys_exit_group kernel/exit.c:1033 [inline] __x64_sys_exit_group+0x3e/0x50 kernel/exit.c:1033 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x39/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7f309be71a09 Code: Unable to access opcode bytes at 0x7f309be719df. RSP: 002b:00007fff171df518 EFLAGS: 00000246 ORIG_RAX: 00000000000000e7 RAX: ffffffffffffffda RBX: 00007f309bef7330 RCX: 00007f309be71a09 RDX: 000000000000003c RSI: 00000000000000e7 RDI: 0000000000000001 RBP: 0000000000000001 R08: fffffffffffffc0 R09: 00007f309bef1e40 R10: 0000000000010600 R11: 0000000000000246 R12: 00007f309bef7330 R13: 0000000000000001 R14: 0000000000000000 R15: 0000000000000001 </TASK> Modules linked in: ---[end trace 0000000000000000]--- RIP: 0010:f2fs_evict_inode+0x172d/0x1e00 fs/f2fs/inode.c:869 Code: ff df 48 c1 ea 03 80 3c 02 00 0f 85 6a 06 00 00 8b 75 40 ba 01 00 00 00 4c 89 e7 e8 6d ce 06 00 e9 aa fc ff ff e8 63 22 e2 fd <0f> 0b e8 5c 22 e2 fd 48 c7 c0 a8 3a 18 8d 48 ba 00 00 00 00 00 fc RSP: 0018:ffffc90003a6fa00 EFLAGS: 00010293 RAX: 0000000000000000 RBX: 0000000000 ---truncated---	N/A	More Details
CVE-2023-53830	In the Linux kernel, the following vulnerability has been resolved: platform/x86: think-lmi: Fix memory leak when showing current settings When retriving a item string with tlmi_setting(), the result has to be freed using kfree(). In current_value_show() however, malformed item strings are not freed, causing a memory leak. Fix this by eliminating the early return responsible for this.	N/A	More Details
CVE-2023-53831	In the Linux kernel, the following vulnerability has been resolved: net: read sk->sk_family once in sk_mc_loop() syzbot is playing with IPV6_ADDRFORM quite a lot these days, and managed to hit the WARN_ON_ONCE(1) in sk_mc_loop() We have many more similar issues to fix. WARNING: CPU: 1 PID: 1593 at net/core/sock.c:782 sk_mc_loop+0x165/0x260 Modules linked in: CPU: 1 PID: 1593 Comm: kworker/1:3 Not tainted 6.1.40-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/26/2023 Workqueue: events_power_efficient gc_worker RIP: 0010:sk_mc_loop+0x165/0x260 net/core/sock.c:782 Code: 34 1b fd 49 81 c7 18 05 00 00 4c 89 f8 48 c1 e8 03 42 80 3c 20 00 74 08 4c 89 ff e8 25 36 6d fd 4d 8b 37 eb 13 e8 db 33 1b fd <0f> 0b b3 01 eb 34 e8 d0 33 1b fd 45 31 f6 49 83 c6 38 4c 89 f0 48 RSP: 0018:ffffc90000388530 EFLAGS: 00010246 RAX: ffffffff846d9b55 RBX: 0000000000000011 RCX: ffff88814f884980 RDX: 0000000000000102 RSI: ffffffff87ae5160 RDI: 0000000000000011 RBP: ffffc90000388550 R08: 0000000000000003 R09: ffffffff846d9a65 R10: 0000000000000002 R11: ffff88814f884980 R12: dffffc0000000000 R13: ffff88810dbee000 R14: 0000000000000010 R15: ffff888150084000 FS: 0000000000000000(0000) GS:ffff8881f6b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000180 CR3: 000000014ee5b000 CR4: 00000000003506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <IRQ> [<ffffffff8507734f>] ip6_finish_output2+0x33f/0x1ae0 net/ipv6/ip6_output.c:83 [<ffffffff85062766>] __ip6_finish_output net/ipv6/ip6_output.c:200 [inline] [<ffffffff85062766>] ip6_finish_output+0x6c6/0xb10 net/ipv6/ip6_output.c:211 [<ffffffff85061f8c>] NF_HOOK_COND include/linux/netfilter.h:298 [inline] [<ffffffff85061f8c>] ip6_output+0x2bc/0x3d0 net/ipv6/ip6_output.c:232 [<ffffffff852071cf>] dst_output include/net/dst.h:444 [inline] [<ffffffff852071cf>] ip6_local_out+0x10f/0x140 net/ipv6/output_core.c:161 [<ffffffff83618fb4>] ipvlan_process_v6_outbound drivers/net/ipvlan/ipvlan_core.c:483 [inline] [<ffffffff83618fb4>] ipvlan_process_outbound drivers/net/ipvlan/ipvlan_core.c:529 [inline] [<ffffffff83618fb4>] ipvlan_xmit_mode_l3 drivers/net/ipvlan/ipvlan_core.c:602 [inline] [<ffffffff83618fb4>] ipvlan_queue_xmit+0x1174/0x1be0 drivers/net/ipvlan/ipvlan_core.c:677 [<ffffffff8361ddd9>] ipvlan_start_xmit+0x49/0x100 drivers/net/ipvlan/ipvlan_main.c:229 [<ffffffff84763fc0>] netdev_start_xmit include/linux/netdevice.h:4925 [inline] [<ffffffff84763fc0>] xmit_one net/core/dev.c:3644 [inline] [<ffffffff84763fc0>] dev_hard_start_xmit+0x320/0x980 net/core/dev.c:3660 [<ffffffff8494c650>] sch_direct_xmit+0x2a0/0x9c0 net/sched/sch_generic.c:342 [<ffffffff8494d883>] qdisc_restart net/sched/sch_generic.c:407 [inline] [<ffffffff8494d883>] __qdisc_run+0xb13/0x1e70 net/sched/sch_generic.c:415 [<ffffffff8478c426>] qdisc_run+0xd6/0x260 include/net/pkt_sched.h:125 [<ffffffff84796eac>] net_tx_action+0x7ac/0x940 net/core/dev.c:5247 [<ffffffff858002bd>] __do_softirq+0x2bd/0x9bd kernel/softirq.c:599 [<ffffffff814c3fe8>] invoke_softirq kernel/softirq.c:430 [inline] [<ffffffff814c3fe8>] __irq_exit_rcu+0xc8/0x170 kernel/softirq.c:683 [<ffffffff814c3f09>] irq_exit_rcu+0x9/0x20 kernel/softirq.c:695	N/A	More Details
CVE-2023-	In the Linux kernel, the following vulnerability has been resolved: md/raid10: fix null-ptr-deref in raid10_sync_request init_resync() inits mempool and sets conf->have_replacemnt at the beginning of sync, close_sync() frees the mempool when sync is completed. After [1] recovery might be skipped and init_resync() is called but close_sync() is not. null-ptr-deref occurs with r10bio->dev[i].repl_bio. The following is one way to reproduce the issue. 1) create a array, wait for resync to complete, mddev->recovery_cp is set to MaxSector. 2) recovery is woken and it is skipped. conf->have_replacement is set to 0 in init_resync(). close_sync() not called. 3) some io errors and rdev	N/A	More Details

53832	A is set to WantReplacement. 4) a new device is added and set to A's replacement. 5) recovery is woken, A have replacement, but conf->have_replacemnt is 0. r10bio->dev[i].repl_bio will not be alloced and null-ptr-deref occurs. Fix it by not calling init_resync() if recovery skipped. [1] commit 7e83ccbecd60 ("md/raid10: Allow skipping recovery when clean arrays are assembled")		
CVE-2023-53833	In the Linux kernel, the following vulnerability has been resolved: drm/i915: Fix NULL ptr deref by checking new_crtc_state intel_atomic_get_new_crtc_state can return NULL, unless crtc state wasn't obtained previously with intel_atomic_get_crtc_state, so we must check it for NULLness here, just as in many other places, where we can't guarantee that intel_atomic_get_crtc_state was called. We are currently getting NULL ptr deref because of that, so this fix was confirmed to help. (cherry picked from commit 1d5b09f8daf859247a1ea65b0d732a24d88980d8)	N/A	More Details
CVE-2023-53834	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ina2xx: avoid NULL pointer dereference on OF device match The affected lines were resulting in a NULL pointer dereference on our platform because the device tree contained the following list of compatible strings: power-sensor@40 { compatible = "ti,ina232", "ti,ina231"; ... }; Since the driver doesn't declare a compatible string "ti,ina232", the OF matching succeeds on "ti,ina231". But the I2C device ID info is populated via the first compatible string, cf. modalias population in of_i2c_get_board_info(). Since there is no "ina232" entry in the legacy I2C device ID table either, the struct i2c_device_id *id pointer in the probe function is NULL. Fix this by using the already populated type variable instead, which points to the proper driver data. Since the name is also wanted, add a generic one to the ina2xx_config table.	N/A	More Details
CVE-2023-53835	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-53836	In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: Fix skb refcnt race after locking changes There is a race where skb's from the sk_psock_backlog can be referenced after userspace side has already skb_consumed() the sk_buff and its refcnt dropped to zer0 causing use after free. The flow is the following: while ((skb = skb_peek(&psock->ingress_skb)) sk_psock_handle_Skb(psock, skb, ..., ingress) if (!ingress) ... sk_psock_skb_ingress sk_psock_skb_ingress_enqueue(skb) msg->skb = skb sk_psock_queue_msg(psock, msg) skb_dequeue(&psock->ingress_skb) The sk_psock_queue_msg() puts the msg on the ingress_msg queue. This is what the application reads when recvmsg() is called. An application can read this anytime after the msg is placed on the queue. The recvmsg hook will also read msg->skb and then after user space reads the msg will call consume_skb(skb) on it effectively free'ing it. But, the race is in above where backlog queue still has a reference to the skb and calls skb_dequeue(). If the skb_dequeue happens after the user reads and free's the skb we have a use after free. The !ingress case does not suffer from this problem because it uses sendmsg_*(sk, msg) which does not pass the sk_buff further down the stack. The following splat was observed with 'test_progs -t sockmap_listen': [1022.710250][T2556] general protection fault, ... [...] [1022.712830][T2556] Workqueue: events sk_psock_backlog [1022.713262][T2556] RIP: 0010:skb_dequeue+0x4c/0x80 [1022.713653][T2556] Code: ... [...] [1022.720699][T2556] Call Trace: [1022.720984][T2556] <TASK> [1022.721254][T2556] ? die_addr+0x32/0x80^M [1022.721589][T2556] ? exc_general_protection+0x25a/0x4b0 [1022.722026][T2556] ? asm_exc_general_protection+0x22/0x30 [1022.722489][T2556] ? skb_dequeue+0x4c/0x80 [1022.722854][T2556] sk_psock_backlog+0x27a/0x300 [1022.723243][T2556] process_one_work+0x2a7/0x5b0 [1022.723633][T2556] worker_thread+0x4f/0x3a0 [1022.723998][T2556] ? __pfx_worker_thread+0x10/0x10 [1022.724386][T2556] kthread+0xfd/0x130 [1022.724709][T2556] ? __pfx_kthread+0x10/0x10 [1022.725066][T2556] ret_from_fork+0x2d/0x50 [1022.725409][T2556] ? __pfx_kthread+0x10/0x10 [1022.725799][T2556] ret_from_fork_asm+0x1b/0x30 [1022.726201][T2556] </TASK> To fix we add an skb_get() before passing the skb to be enqueued in the engress queue. This bumps the skb->users refcnt so that consume_skb() and kfree_skb will not immediately free the sk_buff. With this we can be sure the skb is still around when we do the dequeue. Then we just need to decrement the refcnt or free the skb in the backlog case which we do by calling kfree_skb() on the ingress case as well as the sendmsg case. Before locking change from fixes tag we had the sock locked so we couldn't race with user and there was no issue here.	N/A	More Details
CVE-2023-53837	In the Linux kernel, the following vulnerability has been resolved: drm/msm: fix NULL-deref on snapshot tear down In case of early initialisation errors and on platforms that do not use the DPU controller, the deinitilisation code can be called with the kms pointer set to NULL. Patchwork: https://patchwork.freedesktop.org/patch/525099/	N/A	More Details
CVE-2023-53839	In the Linux kernel, the following vulnerability has been resolved: dccp: fix data-race around dp->dccps_mss_cache dccp_sendmsg() reads dp->dccps_mss_cache before locking the socket. Same thing in do_dccp_getsockopt(). Add READ_ONCE()/WRITE_ONCE() annotations, and change dccp_sendmsg() to check again dccps_mss_cache after socket is locked.	N/A	More Details
CVE-2023-53827	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix use-after-free in l2cap_disconnect_{req,rsp} Similar to commit d0be8347c623 ("Bluetooth: L2CAP: Fix use-after-free caused by l2cap_chan_put"), just use l2cap_chan_hold_unless_zero to prevent referencing a channel that is about to be destroyed.	N/A	More Details
CVE-2023-53840	In the Linux kernel, the following vulnerability has been resolved: usb: early: xhci-dbc: Fix a potential out-of-bound memory access If xdbc_bulk_write() fails, the values in 'buf' can be anything. So the string is not guaranteed to be NULL terminated when xdbc_trace() is called. Reserve an extra byte, which will be zeroed automatically because 'buf' is a static variable, in order to avoid troubles, should it happen.	N/A	More Details
CVE-2023-53841	In the Linux kernel, the following vulnerability has been resolved: devlink: report devlink_port_type_warn source device devlink_port_type_warn is scheduled for port devlink and warning when the port type is not set. But from this warning it is not easy found out which device (driver) has no devlink port set. [3709.975552] Type was not set for devlink port. [3709.975579] WARNING: CPU: 1 PID: 13092 at net/devlink/leftover.c:6775 devlink_port_type_warn+0x11/0x20 [3709.993967] Modules linked in: openvswitch nf_conncount nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 nfnetlink bluetooth rpcsec_gss_krb5 auth_rpcgss nfsv4 dns_resolver nfs lockd grace fscache netfs vhost_net vhost vhost_iotlb tap tun bridge stp llc qrtr intel_rapl_msr intel_rapl_common i10nm_edac nfit libnvdimm x86_pkg_temp_thermal mlx5_ib intel_powerclamp coretemp dell_wmi ledtrig_audio sparse_keymap ipmi_ssif kvm_intel ib_uverbs rfkill ib_core video kvm iTCO_wdt acpi_ipmi intel_vsec irqbypass ipmi_si iTCO_vendor_support dcdbas ipmi_devintf mei_me ipmi_msghandler rapl mei intel_cstate isst_if_mmio isst_if_mbox_pci dell_smbios intel_uncore isst_if_common i2c_i801 dell_wmi_descriptor wmi_bmof i2c_smbus intel_pch_thermal pcspkr acpi_power_meter xfs libcrc32c sd_mod sg nvme_tcp mgag200 i2c_algo_bit nvme_fabrics drm_shmem_helper drm_kms_helper nvme syscopyarea ahci sysfillrect sysimgblt nvme_core fb_sys_fops crct10dif_pclmul libahci mlx5_core sfc crc32_pclmul nvme_common drm [3709.994030] crc32c_intel mtd t10_pi mlxfw libata tg3 mdio megaraid_sas psample ghash_clmulni_intel pci_hyperv_intf wmi dm_multipath sunrpc dm_mirror dm_region_hash dm_log dm_mod be2iscsi bnx2i cnic uio cxgb4i cxgb4 tls libcxgbi libcxgb qla4xxx iscsi_boot_sysfs iscsi_tcp libiscsi_tcp libiscsi scsi_transport_iscsi fuse [3710.108431] CPU: 1 PID: 13092 Comm: kworker/1:1 Kdump: loaded Not tainted 5.14.0-319.el9.x86_64 #1 [3710.108435] Hardware name: Dell Inc. PowerEdge R750/0PJ80M, BIOS 1.8.2 09/14/2022 [3710.108437] Workqueue: events devlink_port_type_warn [3710.108440] RIP: 0010:devlink_port_type_warn+0x11/0x20 [3710.108443] Code: 84 76 fe ff ff 48 c7 03 20 0e 1a ad 31 c0 e9 96 fd ff ff 66 0f 1f 44 00 00 0f 1f 44 00 00 48 c7 c7 18 24 4e ad e8 ef 71 62 ff <0f> 0b c3 cc cc cc cc 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 f6 87 [3710.108445] RSP: 0018:ff3b6d2e8b3c7e90 EFLAGS: 00010282 [3710.108447] RAX: 0000000000000000 RBX: ff366d6580127080 RCX: 0000000000000027 [3710.108448] RDX: 0000000000000027 RSI: 00000000ffff86de RDI: ff366d753f41f8c8 [3710.108449] RBP: ff366d658ff5a0c0 R08: ff366d753f41f8c0 R09: ff3b6d2e8b3c7e18 [3710.108450] R10: 0000000000000001 R11: 0000000000000023 R12: ff366d753f430600 [3710.108451] R13: ff366d753f436900 R14: 0000000000000000 R15: ff366d753f436905 [3710.108452] FS: 0000000000000000(0000)	N/A	More Details

	GS:ff366d753f400000(0000) knlGS:0000000000000000 [3710.108453] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [3710.108454] CR2: 00007f1c57bc74e0 CR3: 000000111d26a001 CR4: 0000000000773ee0 [3710.108456] PKRU: 55555554 [3710.108457] Call Trace: [3710.108458] <TASK> [3710.108459] process_one_work+0x1e2/0x3b0 [3710.108466] ? rescuer_thread+0x390/0x390 [3710.108468] worker_thread+0x50/0x3a0 [3710.108471] ? rescuer_thread+0x390/0x390 [3710.108473] kthread+0xdd/0x100 [3710.108477] ? kthread_complete_and_exit+0x20/0x20 [3710.108479] ret_from_fork+0x1f/0x30 [3710.108485] </TASK> [3710.108486] ---[end trace 1b4b23cd0c65d6a0]--- After patch: [402.473064] ice 0000:41:00.0: Type was not set for devlink port. [402.473064] ice 0000:41:00.1: Type was not set for devlink port.		
CVE-2023-53842	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: wcd-mbhc-v2: fix resource leaks on component remove The MBHC resources must be released on component probe failure and removal so can not be tied to the lifetime of the component device. This is specifically needed to allow probe deferrals of the sound card which otherwise fails when reprobing the codec component: snd-sc8280xp sound: ASoC: failed to instantiate card -517 genirq: Flags mismatch irq 299. 00002001 (mbhc sw intr) vs. 00002001 (mbhc sw intr) wcd938x_codec audio-codec: Failed to request mbhc interrupts -16 wcd938x_codec audio-codec: mbhc initialization failed wcd938x_codec audio-codec: ASoC: error at snd_soc_component_probe on audio-codec: -16 snd-sc8280xp sound: ASoC: failed to instantiate card -16	N/A	More Details
CVE-2023-53843	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: reject negative ifindex Recent changes in net-next (commit 759ab1edb56c ("net: store netdevs in an xarray")) refactored the handling of pre-assigned ifindexes and let syzbot surface a latent problem in ovs. ovs does not validate ifindex, making it possible to create netdev ports with negative ifindex values. It's easy to repro with YNL: $ ./cli.py --spec netlink/specs/ovs_datapath.yaml \ --do new \ --json '{"upcall-pid": 1, "name":"my-dp"}' $ ./cli.py --spec netlink/specs/ovs_vport.yaml \ --do new \ --json '{"upcall-pid": "00000001", "name": "some-port0", "dp-ifindex":3,"ifindex":4294901760,"type":2}' $ ip link show -65536: some-port0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000 link/ether 7a:48:21:ad:0b:fb brd ff:ff:ff:ff:ff:ff ... Validate the inputs. Now the second command correctly returns: $ ./cli.py --spec netlink/specs/ovs_vport.yaml \ --do new \ --json '{"upcall-pid": "00000001", "name": "some-port0", "dp-ifindex":3,"ifindex":4294901760,"type":2}' lib.ynl.NlError: Netlink error: Numerical result out of range nl_len = 108 (92) nl_flags = 0x300 nl_type = 2 error: -34 extack: {'msg': 'integer out of range', 'unknown': [[type:4 len:36] b'\x0c\x00\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0c\x00\x03\x00\xff\xff\xff\x7f\x00\x00\x00\x00\x08\x00\x01\x00\x08\x00\x00\x00'], 'bad-attr': '.ifindex'} Accept 0 since it used to be silently ignored.	N/A	More Details
CVE-2023-53844	In the Linux kernel, the following vulnerability has been resolved: drm/ttm: Don't leak a resource on swapout move error If moving the bo to system for swapout failed, we were leaking a resource. Fix.	N/A	More Details
CVE-2023-53845	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix infinite loop in nilfs_mdt_get_block() If the disk image that nilfs2 mounts is corrupted and a virtual block address obtained by block lookup for a metadata file is invalid, nilfs_bmap_lookup_at_level() may return the same internal return code as -ENOENT, meaning the block does not exist in the metadata file. This duplication of return codes confuses nilfs_mdt_get_block(), causing it to read and create a metadata block indefinitely. In particular, if this happens to the inode metadata file, ifile, semaphore i_rwsem can be left held, causing task hangs in lock_mount. Fix this issue by making nilfs_bmap_lookup_at_level() treat virtual block address translation failures with -ENOENT as metadata corruption instead of returning the error code.	N/A	More Details
CVE-2023-53846	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on direct node in truncate_dnode() syzbot reports below bug: BUG: KASAN: slab-use-after-free in f2fs_truncate_data_blocks_range+0x122a/0x14c0 fs/f2fs/file.c:574 Read of size 4 at addr ffff88802a25c000 by task syz-executor148/5000 CPU: 1 PID: 5000 Comm: syz-executor148 Not tainted 6.4.0-rc7-syzkaller-00041-ge660abd551f1 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/27/2023 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x150 lib/dump_stack.c:106 print_address_description.constprop.0+0x2c/0x3c0 mm/kasan/report.c:351 print_report mm/kasan/report.c:462 [inline] kasan_report+0x11c/0x130 mm/kasan/report.c:572 f2fs_truncate_data_blocks_range+0x122a/0x14c0 fs/f2fs/file.c:574 truncate_dnode+0x229/0x2e0 fs/f2fs/node.c:944 f2fs_truncate_inode_blocks+0x64b/0xde0 fs/f2fs/node.c:1154 f2fs_do_truncate_blocks+0x4ac/0xf30 fs/f2fs/file.c:721 f2fs_truncate_blocks+0x7b/0x300 fs/f2fs/file.c:749 f2fs_truncate.part.0+0x4a5/0x630 fs/f2fs/file.c:799 f2fs_truncate include/linux/fs.h:825 [inline] f2fs_setattr+0x1738/0x2090 fs/f2fs/file.c:1006 notify_change+0xb2c/0x1180 fs/attr.c:483 do_truncate+0x143/0x200 fs/open.c:66 handle_truncate fs/namei.c:3295 [inline] do_open fs/namei.c:3640 [inline] path_openat+0x2083/0x2750 fs/namei.c:3791 do_filp_open+0x1ba/0x410 fs/namei.c:3818 do_sys_openat2+0x16d/0x4c0 fs/open.c:1356 do_sys_open fs/open.c:1372 [inline] __do_sys_creat fs/open.c:1448 [inline] __se_sys_creat fs/open.c:1442 [inline] __x64_sys_creat+0xcd/0x120 fs/open.c:1442 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x39/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd The root cause is, inodeA references inodeB via inodeB's ino, once inodeA is truncated, it calls truncate_dnode() to truncate data blocks in inodeB's node page, it traverse mapping data from node->i.i_addr[0] to node->i.i_addr[ADDRS_PER_BLOCK() - 1], result in out-of-boundary access. This patch fixes to add sanity check on dnode page in truncate_dnode(), so that, it can help to avoid triggering such issue, and once it encounters such issue, it will record newly introduced ERROR_INVALID_NODE_REFERENCE error into superblock, later fsck can detect such issue and try repairing. Also, it removes f2fs_truncate_data_blocks() for cleanup due to the function has only one caller, and uses f2fs_truncate_data_blocks_range() instead.	N/A	More Details
CVE-2023-53847	In the Linux kernel, the following vulnerability has been resolved: usb-storage: alauda: Fix uninit-value in alauda_check_media() Syzbot got KMSAN to complain about access to an uninitialized value in the alauda subdriver of usb-storage: BUG: KMSAN: uninit-value in alauda_transport+0x462/0x57f0 drivers/usb/storage/alauda.c:1137 CPU: 0 PID: 12279 Comm: usb-storage Not tainted 5.3.0-rc7+ #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x191/0x1f0 lib/dump_stack.c:113 kmsan_report+0x13a/0x2b0 mm/kmsan/kmsan_report.c:108 __msan_warning+0x73/0xe0 mm/kmsan/kmsan_instr.c:250 alauda_check_media+0x344/0x3310 drivers/usb/storage/alauda.c:460 The problem is that alauda_check_media() doesn't verify that its USB transfer succeeded before trying to use the received data. What should happen if the transfer fails isn't entirely clear, but a reasonably conservative approach is to pretend that no media is present. A similar problem exists in a usb_stor_dbg() call in alauda_get_media_status(). In this case, when an error occurs the call is redundant, because usb_stor_ctrl_transfer() already will print a debugging message. Finally, unrelated to the uninitialized memory access, is the fact that alauda_check_media() performs DMA to a buffer on the stack. Fortunately usb-storage provides a general purpose DMA-able buffer for uses like this. We'll use it instead.	N/A	More Details
CVE-2023-53848	In the Linux kernel, the following vulnerability has been resolved: md/raid5-cache: fix a deadlock in r5l_exit_log() Commit b13015af94cf ("md/raid5-cache: Clear conf->log after finishing work") introduce a new problem: // caller hold reconfig_mutex r5l_exit_log flush_work(&log->disable_writeback_work) r5c_disable_writeback_async wait_event /* * conf->log is not NULL, and mddev_trylock() * will fail, wait_event() can never pass. */ conf->log = NULL Fix this problem by setting 'config->log' to NULL before wake_up() as it used to be, so that wait_event() from r5c_disable_writeback_async() can exist. In the meantime, move forward md_unregister_thread() so that null-ptr-deref this commit fixed can still be fixed.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: Avoid use-after-free in dbg for hci_add_adv_monitor() KSAN reports use-after-free in hci_add_adv_monitor(). While adding an adv monitor, hci_add_adv_monitor() calls ->		More

2023-53828	msft_add_monitor_pattern() calls -> msft_add_monitor_sync() calls -> msft_le_monitor_advertisement_cb() calls in an error case -> hci_free_adv_monitor() which frees the *moniter. This is referenced by bt_dev_dbg() in hci_add_adv_monitor(). Fix the bt_dev_dbg() by using handle instead of monitor->handle.	N/A	Details
CVE-2023-53826	In the Linux kernel, the following vulnerability has been resolved: ubi: Fix UAF wear-leveling entry in eraseblk_count_seq_show() Wear-leveling entry could be freed in error path, which may be accessed again in eraseblk_count_seq_show(), for example: __erase_worker eraseblk_count_seq_show wl = ubi->lookuptbl[*block_number] if (wl) wl_entry_destroy ubi->lookuptbl[e->pnum] = NULL kmem_cache_free(ubi_wl_entry_slab, e) erase_count = wl->ec // UAF! Wear-leveling entry updating/accessing in ubi->lookuptbl should be protected by ubi->wl_lock, fix it by adding ubi->wl_lock to serialize wl entry accessing between wl_entry_destroy() and eraseblk_count_seq_show(). Fetch a reproducer in [Link].	N/A	More Details
CVE-2022-50664	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: fix leak of memory fw	N/A	More Details
CVE-2022-50674	In the Linux kernel, the following vulnerability has been resolved: riscv: vdso: fix NULL deference in vdso_join_timens() when vfork Testing tools/testing/selftests/timens/vfork_exec.c got below kernel log: [6.838454] Unable to handle kernel access to user memory without uaccess routines at virtual address 0000000000000020 [6.842255] Oops [#1] [6.842871] Modules linked in: [6.844249] CPU: 1 PID: 64 Comm: vfork_exec Not tainted 6.0.0-rc3-rt15+ #8 [6.845861] Hardware name: riscv-virtio,qemu (DT) [6.848009] epc : vdso_join_timens+0xd2/0x110 [6.850097] ra : vdso_join_timens+0xd2/0x110 [6.851164] epc : ffffffff8000635c ra : ffffffff8000635c sp : ff6000000181fbf0 [6.852562] gp : ffffffff80cff648 tp : ff60000000fdb700 t0 : 3030303030303030 [6.853852] t1 : 0000000000000030 t2 : 3030303030303030 s0 : ff6000000181fc40 [6.854984] s1 : ff60000001e6c000 a0 : 0000000000000010 a1 : ffffffff8005654c [6.856221] a2 : 00000000ffffefff a3 : 0000000000000000 a4 : 0000000000000000 [6.858114] a5 : 0000000000000000 a6 : 0000000000000008 a7 : 0000000000000038 [6.859484] s2 : ff60000001e6c068 s3 : ff6000000108abb0 s4 : 0000000000000000 [6.860751] s5 : 0000000000001000 s6 : ffffffff8089dc40 s7 : ffffffff8089dc38 [6.862029] s8 : ffffffff8089dc30 s9 : ff60000000fdbe38 s10: 000000000000005e [6.863304] s11: ffffffff80cc3510 t3 : ffffffff80d1112f t4 : ffffffff80d1112f [6.864565] t5 : ffffffff80d11130 t6 : ff6000000181fa00 [6.865561] status: 0000000000000120 badaddr: 0000000000000020 cause: 000000000000000d [6.868046] [<ffffffff8008dc94>] timens_commit+0x38/0x11a [6.869089] [<ffffffff8008dde8>] timens_on_fork+0x72/0xb4 [6.870055] [<ffffffff80190096>] begin_new_exec+0x3c6/0x9f0 [6.871231] [<ffffffff801d826c>] load_elf_binary+0x628/0x1214 [6.872304] [<ffffffff8018ee7a>] bprm_execve+0x1f2/0x4e4 [6.873243] [<ffffffff8018f90c>] do_execveat_common+0x16e/0x1ee [6.874258] [<ffffffff8018f9c8>] sys_execve+0x3c/0x48 [6.875162] [<ffffffff80003556>] ret_from_syscall+0x0/0x2 [6.877484] ---[end trace 0000000000000000]--- This is because the mm->context.vdso_info is NULL in vfork case. From another side, mm->context.vdso_info either points to vdso info for RV64 or vdso info for compat, there's no need to bloat riscv's mm_context_t, we can handle the difference when setup the additional page for vdso.	N/A	More Details
CVE-2022-50665	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix failed to find the peer with peer_id 0 when disconnected It has a fail log which is ath11k_dbg in ath11k_dp_rx_process_mon_status(), as below, it will not print when debug_mask is not set ATH11K_DBG_DATA. ath11k_dbg(ab, ATH11K_DBG_DATA, "failed to find the peer with peer_id %d\n", ppdu_info.peer_id); When run scan with station disconnected, the peer_id is 0 for case HAL_RX_MPDU_START in ath11k_hal_rx_parse_mon_status_tlv() which called from ath11k_dp_rx_process_mon_status(), and the peer_id of ppdu_info is reset to 0 in the while loop, so it does not match condition of the check "if (ppdu_info->peer_id == HAL_INVALID_PEERID" in the loop, and then the log "failed to find the peer with peer_id 0" print after the check in the loop, it is below call stack when debug_mask is set ATH11K_DBG_DATA. The reason is this commit 01d2f285e3e5 ("ath11k: decode HE status tlv") add "memset(ppdu_info, 0, sizeof(struct hal_rx_mon_ppdu_info))" in ath11k_dp_rx_process_mon_status(), but the commit does not initialize the peer_id to HAL_INVALID_PEERID, then lead the check mis-match. Callstack of the failed log: [12335.689072] RIP: 0010:ath11k_dp_rx_process_mon_status+0x9ea/0x1020 [ath11k] [12335.689157] Code: 89 ff e8 f9 10 00 00 be 01 00 00 00 4c 89 f7 e8 dc 4b 4e de 48 8b 85 38 ff ff ff c7 80 e4 07 00 00 01 00 00 00 e9 20 f8 ff ff <0f> 0b 41 0f b7 96 be 06 00 00 48 c7 c6 b8 50 44 c1 4c 89 ff e8 fd [12335.689180] RSP: 0018:ffffb874001a4ca0 EFLAGS: 00010246 [12335.689210] RAX: 0000000000000000 RBX: ffff995642cbd100 RCX: 0000000000000000 [12335.689229] RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff99564212cd18 [12335.689248] RBP: ffffb874001a4dc0 R08: 0000000000000001 R09: 0000000000000000 [12335.689268] R10: 0000000000000220 R11: ffffb874001a48e8 R12: ffff995642473d40 [12335.689286] R13: ffff99564212c5b8 R14: ffff9956424736a0 R15: ffff995642120000 [12335.689303] FS: 0000000000000000(0000) GS:ffff995739000000(0000) knlGS:0000000000000000 [12335.689323] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [12335.689341] CR2: 00007f43c5d5e039 CR3: 000000011c012005 CR4: 00000000000606e0 [12335.689360] Call Trace: [12335.689377] <IRQ> [12335.689418] ? rcu_read_lock_held_common+0x12/0x50 [12335.689447] ? rcu_read_lock_sched_held+0x25/0x80 [12335.689471] ? rcu_read_lock_held_common+0x12/0x50 [12335.689504] ath11k_dp_rx_process_mon_rings+0x8d/0x4f0 [ath11k] [12335.689578] ? ath11k_dp_rx_process_mon_rings+0x8d/0x4f0 [ath11k] [12335.689653] ? lock_acquire+0xef/0x360 [12335.689681] ? rcu_read_lock_sched_held+0x25/0x80 [12335.689713] ath11k_dp_service_mon_ring+0x38/0x60 [ath11k] [12335.689784] ? ath11k_dp_rx_process_mon_rings+0x4f0/0x4f0 [ath11k] [12335.689860] call_timer_fn+0xb2/0x2f0 [12335.689897] ? ath11k_dp_rx_process_mon_rings+0x4f0/0x4f0 [ath11k] [12335.689970] run_timer_softirq+0x21f/0x540 [12335.689999] ? ktime_get+0xad/0x160 [12335.690025] ? lapic_next_deadline+0x2c/0x40 [12335.690053] ? clockevents_program_event+0x82/0x100 [12335.690093] __do_softirq+0x151/0x4a8 [12335.690135] irq_exit_rcu+0xc9/0x100 [12335.690165] sysvec_apic_timer_interrupt+0xa8/0xd0 [12335.690189] </IRQ> [12335.690204] <TASK> [12335.690225] asm_sysvec_apic_timer_interrupt+0x12/0x20 Reset the default value to HAL_INVALID_PEERID each time after memset of ppdu_info as well as others memset which existed in function ath11k_dp_rx_process_mon_status(), then the failed log disappeared. Tested-on: WCN6855 hw2.0 PCI WLAN.HSP.1.1-03125-QCAHSPSWPL_V1_V2_SILICONZ_LITE-3	N/A	More Details
CVE-2022-50666	In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: Fix QP destroy to wait for all references dropped. Delay QP destroy completion until all siw references to QP are dropped. The calling RDMA core will free QP structure after successful return from siw_qp_destroy() call, so siw must not hold any remaining reference to the QP upon return. A use-after-free was encountered in xfstest generic/460, while testing NFSoRDMA. Here, after a TCP connection drop by peer, the triggered siw_cm_work_handler got delayed until after QP destroy call, referencing a QP which has already freed.	N/A	More Details
CVE-2022-50667	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix memory leak in vmw_mksstat_add_ioctl() If the copy of the description string from userspace fails, then the page for the instance descriptor doesn't get freed before returning -EFAULT, which leads to a memleak.	N/A	More Details
CVE-2022-50668	In the Linux kernel, the following vulnerability has been resolved: ext4: fix deadlock due to mbcache entry corruption When manipulating xattr blocks, we can deadlock infinitely looping inside ext4_xattr_block_set() where we constantly keep finding xattr block for reuse in mbcache but we are unable to reuse it because its reference count is too big. This happens because cache entry for the xattr block is marked as reusable (e_reusable set) although its reference count is too big. When this inconsistency happens, this inconsistent state is kept indefinitely and so ext4_xattr_block_set() keeps retrying indefinitely. The inconsistent state is caused by non-atomic update of e_reusable bit. e_reusable is part of a bitfield and e_reusable update can race with update of e_referenced bit in the same bitfield resulting in loss of one of the updates. Fix the problem by using atomic bitops instead. This bug has been around for many years, but it became *much* easier to hit after commit 65f8b80053a1 ("ext4: fix race when reusing xattr blocks").	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: misc: ocxl: fix possible name leak in ocxl_file_register_afu() If		

2022-50669	device_register() returns error in ocxl_file_register_afu(), the name allocated by dev_set_name() need be freed. As comment of device_register() says, it should use put_device() to give up the reference in the error path. So fix this by calling put_device(), then the name can be freed in kobject_cleanup(), and info is freed in info_release().	N/A	More Details
CVE-2022-50670	In the Linux kernel, the following vulnerability has been resolved: mmc: omap_hsmmc: fix return value check of mmc_add_host() mmc_add_host() may return error, if we ignore its return value, it will lead two issues: 1. The memory that allocated in mmc_alloc_host() is leaked. 2. In the remove() path, mmc_remove_host() will be called to delete device, but it's not added yet, it will lead a kernel crash because of null-ptr-deref in device_del(). Fix this by checking the return value and goto error path wihch will call mmc_free_host().	N/A	More Details
CVE-2022-50671	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix "kernel NULL pointer dereference" error When rxe_queue_init in the function rxe_qp_init_req fails, both qp->req.task.func and qp->req.task.arg are not initialized. Because of creation of qp fails, the function rxe_create_qp will call rxe_qp_do_cleanup to handle allocated resource. Before calling __rxe_do_task, both qp->req.task.func and qp->req.task.arg should be checked.	N/A	More Details
CVE-2022-50672	In the Linux kernel, the following vulnerability has been resolved: mailbox: zynq-ipi: fix error handling while device_register() fails If device_register() fails, it has two issues: 1. The name allocated by dev_set_name() is leaked. 2. The parent of device is not NULL, device_unregister() is called in zynqmp_ipi_free_mboxes(), it will lead a kernel crash because of removing not added device. Call put_device() to give up the reference, so the name is freed in kobject_cleanup(). Add device registered check in zynqmp_ipi_free_mboxes() to avoid null-ptr-deref.	N/A	More Details
CVE-2022-50673	In the Linux kernel, the following vulnerability has been resolved: ext4: fix use-after-free in ext4_orphan_cleanup I caught a issue as follows: == BUG: KASAN: use-after-free in __list_add_valid+0x28/0x1a0 Read of size 8 at addr ffff88814b13f378 by task mount/710 CPU: 1 PID: 710 Comm: mount Not tainted 6.1.0-rc3-next #370 Call Trace: <TASK> dump_stack_lvl+0x73/0x9f print_report+0x25d/0x759 kasan_report+0xc0/0x120 __asan_load8+0x99/0x140 __list_add_valid+0x28/0x1a0 ext4_orphan_cleanup+0x564/0x9d0 [ext4] __ext4_fill_super+0x48e2/0x5300 [ext4] ext4_fill_super+0x19f/0x3a0 [ext4] get_tree_bdev+0x27b/0x450 ext4_get_tree+0x19/0x30 [ext4] vfs_get_tree+0x49/0x150 path_mount+0xaae/0x1350 do_mount+0xe2/0x110 __x64_sys_mount+0xf0/0x190 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd </TASK> [...] == Above issue may happen as follows: ---------- ext4_fill_super ext4_orphan_cleanup --- loop1: assume last_orphan is 12 --- list_add(&EXT4_I(inode)->i_orphan, &EXT4_SB(sb)->s_orphan) ext4_truncate --> return 0 ext4_inode_attach_jinode --> return -ENOMEM iput(inode) --> free inode<12> --- loop2: last_orphan is still 12 --- list_add(&EXT4_I(inode)->i_orphan, &EXT4_SB(sb)->s_orphan); // use inode<12> and trigger UAF To solve this issue, we need to propagate the return value of ext4_inode_attach_jinode() appropriately.	N/A	More Details
CVE-2022-50675	In the Linux kernel, the following vulnerability has been resolved: arm64: mte: Avoid setting PG_mte_tagged if no tags cleared or restored Prior to commit 69e3b846d8a7 ("arm64: mte: Sync tags for pages where PTE is untagged"), mte_sync_tags() was only called for pte_tagged() entries (those mapped with PROT_MTE). Therefore mte_sync_tags() could safely use test_and_set_bit(PG_mte_tagged, &page->flags) without inadvertently setting PG_mte_tagged on an untagged page. The above commit was required as guests may enable MTE without any control at the stage 2 mapping, nor a PROT_MTE mapping in the VMM. However, the side-effect was that any page with a PTE that looked like swap (or migration) was getting PG_mte_tagged set automatically. A subsequent page copy (e.g. migration) copied the tags to the destination page even if the tags were owned by KASAN. This issue was masked by the page_kasan_tag_reset() call introduced in commit e5b8d9218951 ("arm64: mte: reset the page tag in page->flags"). When this commit was reverted (20794545c146), KASAN started reporting access faults because the overriding tags in a page did not match the original page->flags (with CONFIG_KASAN_HW_TAGS=y): BUG: KASAN: invalid-access in copy_page+0x10/0xd0 arch/arm64/lib/copy_page.S:26 Read at addr f5ff000017f2e000 by task syz-executor.1/2218 Pointer tag: [f5], memory tag: [f2] Move the PG_mte_tagged bit setting from mte_sync_tags() to the actual place where tags are cleared (mte_sync_page_tags()) or restored (mte_restore_tags()).	N/A	More Details
CVE-2023-53825	In the Linux kernel, the following vulnerability has been resolved: kcm: Fix error handling for SOCK_DGRAM in kcm_sendmsg(). syzkaller found a memory leak in kcm_sendmsg(), and commit c821a88bd720 ("kcm: Fix memory leak in error path of kcm_sendmsg()") suppressed it by updating kcm_tx_msg(head)->last_skb if partial data is copied so that the following sendmsg() will resume from the skb. However, we cannot know how many bytes were copied when we get the error. Thus, we could mess up the MSG_MORE queue. When kcm_sendmsg() fails for SOCK_DGRAM, we should purge the queue as we do so for UDP by udp_flush_pending_frames(). Even without this change, when the error occurred, the following sendmsg() resumed from a wrong skb and the queue was messed up. However, we have yet to get such a report, and only syzkaller stumbled on it. So, this can be changed safely. Note this does not change SOCK_SEQPACKET behaviour.	N/A	More Details
CVE-2022-50676	In the Linux kernel, the following vulnerability has been resolved: net: rds: don't hold sock lock when cancelling work from rds_tcp_reset_callbacks() syzbot is reporting lockdep warning at rds_tcp_reset_callbacks() [1], for commit ac3615e7f3cffe2a ("RDS: TCP: Reduce code duplication in rds_tcp_reset_callbacks()") added cancel_delayed_work_sync() into a section protected by lock_sock() without realizing that rds_send_xmit() might call lock_sock(). We don't need to protect cancel_delayed_work_sync() using lock_sock(), for even if rds_{send,recv}_worker() re-queued this work while __flush_work() from cancel_delayed_work_sync() was waiting for this work to complete, retried rds_{send,recv}_worker() is no-op due to the absence of RDS_CONN_UP bit.	N/A	More Details
CVE-2022-50677	In the Linux kernel, the following vulnerability has been resolved: ipmi: fix use after free in _ipmi_destroy_user() The intf_free() function frees the "intf" pointer so we cannot dereference it again on the next line.	N/A	More Details
CVE-2022-50678	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: fix invalid address access when enabling SCAN log level The variable i is changed when setting random MAC address and causes invalid address access when printing the value of pi->reqs[i]->reqid. We replace reqs index with ri to fix the issue. [136.726473] Unable to handle kernel access to user memory outside uaccess routines at virtual address 0000000000000000 [136.737365] Mem abort info: [136.740172] ESR = 0x96000004 [136.743359] Exception class = DABT (current EL), IL = 32 bits [136.749294] SET = 0, FnV = 0 [136.752481] EA = 0, S1PTW = 0 [136.755635] Data abort info: [136.758514] ISV = 0, ISS = 0x00000004 [136.762487] CM = 0, WnR = 0 [136.765522] user pgtable: 4k pages, 48-bit VAs, pgdp = 000000005c4e2577 [136.772265] [0000000000000000] pgd=0000000000000000 [136.777160] Internal error: Oops: 96000004 [#1] PREEMPT SMP [136.782732] Modules linked in: brcmfmac(O) brcmutil(O) cfg80211(O) compat(O) [136.789788] Process wificond (pid: 3175, stack limit = 0x00000000053048fb) [136.796664] CPU: 3 PID: 3175 Comm: wificond Tainted: G O 4.19.42-00001-g531a5f5 #1 [136.805532] Hardware name: Freescale i.MX8MQ EVK (DT) [136.810584] pstate: 60400005 (nZCv daif +PAN -UAO) [136.815429] pc : brcmf_pno_config_sched_scans+0x6cc/0xa80 [brcmfmac] [136.821811] lr : brcmf_pno_config_sched_scans+0x67c/0xa80 [brcmfmac] [136.828162] sp : ffff00000e9a3880 [136.831475] x29: ffff00000e9a3890 x28: ffff800020543400 [136.836786] x27: ffff8000b1008880 x26: ffff0000012bf6a0 [136.842098] x25: ffff80002054345c x24: ffff800088d22400 [136.847409] x23: ffff0000012bf638 x22: ffff0000012bf6d8 [136.852721] x21: ffff8000aced8fc0 x20: ffff8000ac164400 [136.858032] x19: ffff00000e9a3946 x18: 0000000000000000 [136.863343] x17: 0000000000000000 x16: 0000000000000000 [136.868655] x15: ffff0000093f3b37 x14: 0000000000000050 [136.873966] x13: 0000000000003135 x12: 0000000000000000 [136.879277] x11: 0000000000000000 x10: ffff000009a61888 [136.884589] x9 : 000000000000000f x8 : 0000000000000008 [136.889900] x7 : 303a32303d726464 x6 : ffff00000a1f957d [136.895211] x5 : 0000000000000000 x4 : ffff00000e9a3942 [136.900523] x3 : 0000000000000000 x2 : ffff0000012cead8 [136.905834] x1 : ffff0000012bf6d8 x0 : 0000000000000000 [136.911146] Call trace: [136.913623] brcmf_pno_config_sched_scans+0x6cc/0xa80 [brcmfmac] [136.919658] brcmf_pno_start_sched_scan+0xa4/0x118 [brcmfmac] [	N/A	More Details

	136.925430] brcmf_cfg80211_sched_scan_start+0x80/0xe0 [brcmfmac] [136.931636] nl80211_start_sched_scan+0x140/0x308 [cfg80211] [136.937298] genl_rcv_msg+0x358/0x3f4 [136.940960] netlink_rcv_skb+0xb4/0x118 [136.944795] genl_rcv+0x34/0x48 [136.947935] netlink_unicast+0x264/0x300 [136.951856] netlink_sendmsg+0x2e4/0x33c [136.955781] __sys_sendto+0x120/0x19c		
CVE-2022-50679	In the Linux kernel, the following vulnerability has been resolved: i40e: Fix DMA mappings leak During reallocation of RX buffers, new DMA mappings are created for those buffers. steps for reproduction: while : do for ((i=0; i<=8160; i=i+32)) do ethtool -G enp130s0f0 rx $i tx $i sleep 0.5 ethtool -g enp130s0f0 done done This resulted in crash: i40e 0000:01:00.1: Unable to allocate memory for the Rx descriptor ring, size=65536 Driver BUG WARNING: CPU: 0 PID: 4300 at net/core/xdp.c:141 xdp_rxq_info_unreg+0x43/0x50 Call Trace: i40e_free_rx_resources+0x70/0x80 [i40e] i40e_set_ringparam+0x27c/0x800 [i40e] ethnl_set_rings+0x1b2/0x290 genl_family_rcv_msg_doit.isra.15+0x10f/0x150 genl_family_rcv_msg+0xb3/0x160 ? rings_fill_reply+0x1a0/0x1a0 genl_rcv_msg+0x47/0x90 ? genl_family_rcv_msg+0x160/0x160 netlink_rcv_skb+0x4c/0x120 genl_rcv+0x24/0x40 netlink_unicast+0x196/0x230 netlink_sendmsg+0x204/0x3d0 sock_sendmsg+0x4c/0x50 __sys_sendto+0xee/0x160 ? handle_mm_fault+0xbe/0x1e0 ? syscall_trace_enter+0x1d3/0x2c0 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x5b/0x1a0 entry_SYSCALL_64_after_hwframe+0x65/0xca RIP: 0033:0x7f5eac8b035b Missing register, driver bug WARNING: CPU: 0 PID: 4300 at net/core/xdp.c:119 xdp_rxq_info_unreg_mem_model+0x69/0x140 Call Trace: xdp_rxq_info_unreg+0x1e/0x50 i40e_free_rx_resources+0x70/0x80 [i40e] i40e_set_ringparam+0x27c/0x800 [i40e] ethnl_set_rings+0x1b2/0x290 genl_family_rcv_msg_doit.isra.15+0x10f/0x150 genl_family_rcv_msg+0xb3/0x160 ? rings_fill_reply+0x1a0/0x1a0 genl_rcv_msg+0x47/0x90 ? genl_family_rcv_msg+0x160/0x160 netlink_rcv_skb+0x4c/0x120 genl_rcv+0x24/0x40 netlink_unicast+0x196/0x230 netlink_sendmsg+0x204/0x3d0 sock_sendmsg+0x4c/0x50 __sys_sendto+0xee/0x160 ? handle_mm_fault+0xbe/0x1e0 ? syscall_trace_enter+0x1d3/0x2c0 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x5b/0x1a0 entry_SYSCALL_64_after_hwframe+0x65/0xca RIP: 0033:0x7f5eac8b035b This was caused because of new buffers with different RX ring count should substitute older ones, but those buffers were freed in i40e_configure_rx_ring and reallocated again with i40e_alloc_rx_bi, thus kfree on rx_bi caused leak of already mapped DMA. Fix this by reallocating ZC with rx_bi_zc struct when BPF program loads. Additionally reallocate back to rx_bi when BPF program unloads. If BPF program is loaded/unloaded and XSK pools are created, reallocate RX queues accordingly in XSP_SETUP_XSK_POOL handler.	N/A	More Details
CVE-2023-53820	In the Linux kernel, the following vulnerability has been resolved: loop: loop_set_status_from_info() check before assignment In loop_set_status_from_info(), lo->lo_offset and lo->lo_sizelimit should be checked before reassignment, because if an overflow error occurs, the original correct value will be changed to the wrong value, and it will not be changed back. More, the original patch did not solve the problem, the value was set and ioctl returned an error, but the subsequent io used the value in the loop driver, which still caused an alarm: loop_handle_cmd do_req_filebacked loff_t pos = ((loff_t) blk_rq_pos(rq) << 9) + lo->lo_offset; lo_rw_aio cmd->iocb.ki_pos = pos	N/A	More Details
CVE-2023-53821	In the Linux kernel, the following vulnerability has been resolved: ip6_vti: fix slab-use-after-free in decode_session6 When ipv6_vti device is set to the qdisc of the sfb type, the cb field of the sent skb may be modified during enqueuing. Then, slab-use-after-free may occur when ipv6_vti device sends IPv6 packets. The stack information is as follows: BUG: KASAN: slab-use-after-free in decode_session6+0x103f/0x1890 Read of size 1 at addr ffff88802e08edc2 by task swapper/0/0 CPU: 0 PID: 0 Comm: swapper/0 Not tainted 6.4.0-next-20230707-00001-g84e2cad7f979 #410 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-1.fc33 04/01/2014 Call Trace: <IRQ> dump_stack_lvl+0xd9/0x150 print_address_description.constprop.0+0x2c/0x3c0 kasan_report+0x11d/0x130 decode_session6+0x103f/0x1890 __xfrm_decode_session+0x54/0xb0 vti6_tnl_xmit+0x3e6/0x1ee0 dev_hard_start_xmit+0x187/0x700 sch_direct_xmit+0x1a3/0xc30 __qdisc_run+0x510/0x17a0 __dev_queue_xmit+0x2215/0x3b10 neigh_connected_output+0x3c2/0x550 ip6_finish_output2+0x55a/0x1550 ip6_finish_output+0x6b9/0x1270 ip6_output+0x1f1/0x540 ndisc_send_skb+0xa63/0x1890 ndisc_send_rs+0x132/0x6f0 addrconf_rs_timer+0x3f1/0x870 call_timer_fn+0x1a0/0x580 expire_timers+0x29b/0x4b0 run_timer_softirq+0x326/0x910 __do_softirq+0x1d4/0x905 irq_exit_rcu+0xb7/0x120 sysvec_apic_timer_interrupt+0x97/0xc0 </IRQ> Allocated by task 9176: kasan_save_stack+0x22/0x40 kasan_set_track+0x25/0x30 __kasan_slab_alloc+0x7f/0x90 kmem_cache_alloc_node+0x1cd/0x410 kmalloc_reserve+0x165/0x270 __alloc_skb+0x129/0x330 netlink_sendmsg+0x9b1/0xe30 sock_sendmsg+0xde/0x190 ____sys_sendmsg+0x739/0x920 ___sys_sendmsg+0x110/0x1b0 __sys_sendmsg+0xf7/0x1c0 do_syscall_64+0x39/0xb0 entry_SYSCALL_64_after_hwframe+0x63/0xcd Freed by task 9176: kasan_save_stack+0x22/0x40 kasan_set_track+0x25/0x30 kasan_save_free_info+0x2b/0x40 ____kasan_slab_free+0x160/0x1c0 slab_free_freelist_hook+0x11b/0x220 kmem_cache_free+0xf0/0x490 skb_free_head+0x17f/0x1b0 skb_release_data+0x59c/0x850 consume_skb+0xd2/0x170 netlink_unicast+0x54f/0x7f0 netlink_sendmsg+0x926/0xe30 sock_sendmsg+0xde/0x190 ____sys_sendmsg+0x739/0x920 ___sys_sendmsg+0x110/0x1b0 __sys_sendmsg+0xf7/0x1c0 do_syscall_64+0x39/0xb0 entry_SYSCALL_64_after_hwframe+0x63/0xcd The buggy address belongs to the object at ffff88802e08ed00 which belongs to the cache skbuff_small_head of size 640 The buggy address is located 194 bytes inside of freed 640-byte region [ffff88802e08ed00, ffff88802e08ef80) As commit f855691975bb ("xfrm6: Fix the nexthdr offset in _decode_session6.") showed, xfrm_decode_session was originally intended only for the receive path. IP6CB(skb)->nhoff is not set during transmission. Therefore, set the cb field in the skb to 0 before sending packets.	N/A	More Details
CVE-2023-53822	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: Ignore frags from uninitialized peer in dp. When max virtual ap interfaces are configured in all the bands with ACS and hostapd restart is done every 60s, a crash is observed at random times. In this certain scenario, a fragmented packet is received for self peer, for which rx_tid and rx_frags are not initialized in datapath. While handling this fragment, crash is observed as the rx_frag list is uninitialised and when we walk in ath11k_dp_rx_h_sort_frags, skb null leads to exception. To address this, before processing received fragments we check dp_setup_done flag is set to ensure that peer has completed its dp peer setup for fragment queue, else ignore processing the fragments. Call trace: ath11k_dp_process_rx_err+0x550/0x1084 [ath11k] ath11k_dp_service_srng+0x70/0x370 [ath11k] 0xffffffc009693a04 __napi_poll+0x30/0xa4 net_rx_action+0x118/0x270 __do_softirq+0x10c/0x244 irq_exit+0x64/0xb4 __handle_domain_irq+0x88/0xac gic_handle_irq+0x74/0xbc el1_irq+0xf0/0x1c0 arch_cpu_idle+0x10/0x18 do_idle+0x104/0x248 cpu_startup_entry+0x20/0x64 rest_init+0xd0/0xdc arch_call_rest_init+0xc/0x14 start_kernel+0x480/0x4b8 Code: f9400281 f94066a2 91405021 b94a0023 (f9406401) Tested-on: IPQ8074 hw2.0 AHB WLAN.HK.2.7.0.1-01744-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2023-53823	In the Linux kernel, the following vulnerability has been resolved: block/rq_qos: protect rq_qos apis with a new lock commit 50e34d78815e ("block: disable the elevator int del_gendisk") move rq_qos_exit() from disk_release() to del_gendisk(), this will introduce some problems: 1) If rq_qos_add() is triggered by enabling iocost/iolatency through cgroupfs, then it can concurrent with del_gendisk(), it's not safe to write 'q->rq_qos' concurrently. 2) Activate cgroup policy that is relied on rq_qos will call rq_qos_add() and blkcg_activate_policy(), and if rq_qos_exit() is called in the middle, null-ptr-dereference will be triggered in blkcg_activate_policy(). 3) blkg_conf_open_bdev() can call blkdev_get_no_open() first to find the disk, then if rq_qos_exit() from del_gendisk() is done before rq_qos_add(), then memory will be leaked. This patch add a new disk level mutex 'rq_qos_mutex': 1) The lock will protect rq_qos_exit() directly. 2) For wbt that doesn't relied on blk-cgroup, rq_qos_add() can only be called from disk initialization for now because wbt can't be destructed until rq_qos_exit(), so it's safe not to protect wbt for now. Hoever, in case that rq_qos dynamically destruction is supported in the furture, this patch also protect rq_qos_add() from wbt_init() directly, this is enough because blk-sysfs already synchronize writers with disk removal. 3) For iocost and iolatency, in order to synchronize disk removal and cgroup configuration, the lock is held after blkdev_get_no_open() from blkg_conf_open_bdev(), and is released in blkg_conf_exit(). In order to fix the above memory leak, disk_live() is checked after holding the new lock.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: netlink: annotate lockless accesses to nlk->max_recvmsg_len syzbot reported a data-race in data-race in netlink_recvmsg() [1] Indeed, netlink_recvmsg() can be run concurrently, and netlink_dump() also		

CVE-2023-53824	needs protection. [1] BUG: KCSAN: data-race in netlink_recvmsg / netlink_recvmsg read to 0xffff888141840b38 of 8 bytes by task 23057 on cpu 0: netlink_recvmsg+0xea/0x730 net/netlink/af_netlink.c:1988 sock_recvmsg_nosec net/socket.c:1017 [inline] sock_recvmsg net/socket.c:1038 [inline] __sys_recvfrom+0x1ee/0x2e0 net/socket.c:2194 __do_sys_recvfrom net/socket.c:2212 [inline] __se_sys_recvfrom net/socket.c:2208 [inline] __x64_sys_recvfrom+0x78/0x90 net/socket.c:2208 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 write to 0xffff888141840b38 of 8 bytes by task 23037 on cpu 1: netlink_recvmsg+0x114/0x730 net/netlink/af_netlink.c:1989 sock_recvmsg_nosec net/socket.c:1017 [inline] sock_recvmsg net/socket.c:1038 [inline] ____sys_recvmsg+0x156/0x310 net/socket.c:2720 ___sys_recvmsg net/socket.c:2762 [inline] do_recvmmsg+0x2e5/0x710 net/socket.c:2856 __sys_recvmmsg net/socket.c:2935 [inline] __do_sys_recvmmsg net/socket.c:2958 [inline] __se_sys_recvmmsg net/socket.c:2951 [inline] __x64_sys_recvmmsg+0xe2/0x160 net/socket.c:2951 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: 0x0000000000000000 -> 0x0000000000001000 Reported by Kernel Concurrency Sanitizer on: CPU: 1 PID: 23037 Comm: syz-executor.2 Not tainted 6.3.0-rc4-syzkaller-00195-g5a57b48fdfcb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/02/2023	N/A	More Details
CVE-2025-67498	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Details