SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 30 July 2025

Generated on 30 July 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-2025-41240	Three Bitnami Helm charts mount Kubernetes Secrets under a predictable path (/opt/bitnami/*/secrets) that is located within the web server document root. In affected versions, this can lead to unauthenticated access to sensitive credentials via HTTP/S. A remote attacker could retrieve these secrets by accessing specific URLs if the application is exposed externally. The issue affects deployments using the default value of usePasswordFiles=true, which mounts secrets as files into the container filesystem.	10.0	More Details
CVE-2025-54419	A SAML library not dependent on any frameworks that runs in Node. In version 5.0.1, Node-SAML loads the assertion from the (unsigned) original response document. This is different than the parts that are verified when checking signature. This allows an attacker to modify authentication details within a valid SAML assertion. For example, in one attack it is possible to remove any character from the SAML assertion username. To conduct the attack an attacker would need a validly signed document from the identity provider (IdP). This is fixed in version 5.1.0.	10.0	More Details
CVE-2025-5243	Unrestricted Upload of File with Dangerous Type, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in SMG Software Information Portal allows Code Injection, Upload a Web Shell to a Web Server, Code Inclusion.This issue affects Information Portal: before 13.06.2025.	10.0	More Details
CVE-2025-54381	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. In versions 1.4.0 until 1.4.19, the file upload processing system contains an SSRF vulnerability that allows unauthenticated remote attackers to force the server to make arbitrary HTTP requests. The vulnerability stems from the multipart form data and JSON request handlers, which automatically download files from user-provided URLs without validating whether those URLs point to internal network addresses, cloud metadata endpoints, or other restricted resources. The documentation explicitly promotes this URL-based file upload feature, making it an intended design that exposes all deployed services to SSRF attacks by default. Version 1.4.19 contains a patch for the issue.	9.9	More Details
CVE-2025-29631	An issue in Gardyn 4 allows a remote attacker execute arbitrary code	9.8	More Details
CVE-2025-54440	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-6260	The embedded web server on the thermostat listed version ranges contain a vulnerability that allows unauthenticated attackers, either on the local area network or from the Internet via a router with port forwarding set up, to gain direct access to the thermostat's embedded web server and reset user credentials by manipulating specific elements of the embedded web interface.	9.8	More Details
CVE-2015-10143	The Platform theme for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the *_ajax_save_options() function in all versions up to 1.4.4 (exclusive). This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	9.8	More Details
CVE-2019-25224	The WP Database Backup plugin for WordPress is vulnerable to OS Command Injection in versions before 5.2 via the mysqldump function. This vulnerability allows unauthenticated attackers to execute arbitrary commands on the host operating system.	9.8	More Details

CVE-2025-45777	An issue in the OTP mechanism of Chavara Family Welfare Centre Chavara Matrimony Site v2.0 allows attackers to bypass authentication via supplying a crafted request.	9.8	More Details
CVE-2025-6895	The Melapress Login Security plugin for WordPress is vulnerable to Authentication Bypass due to missing authorization within the get_valid_user_based_on_token() function in versions 2.1.0 to 2.1.1. This makes it possible for unauthenticated attackers who know an arbitrary user meta value to bypass authentication checks and log in as that user.	9.8	More Details
CVE-2025-46199	Cross Site Scripting vulnerability in grav v.1.7.48 and before allows an attacker to execute arbitrary code via a crafted script to the form fields	9.8	More Details
CVE-2025-6918	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ncvav Virtual PBX Software allows SQL Injection.This issue affects Virtual PBX Software: before 09.07.2025.	9.8	More Details
CVE-2025-54418	CodeIgniter is a PHP full-stack web framework. A command injection vulnerability present in versions prior to 4.6.2 affects applications that use the ImageMagick handler for image processing (`imagick` as the image library) and either allow file uploads with user-controlled filenames and process uploaded images using the `resize()` method or use the `text()` method with user-controlled text content or options. An attacker can upload a file with a malicious filename containing shell metacharacters that get executed when the image is processed or provide malicious text content or options that get executed when adding text to images Users should upgrade to v4.6.2 or later to receive a patch. As a workaround, switch to the GD image handler (`gd`, the default handler), which is not affected by either vulnerability. For file upload scenarios, instead of using user-provided filenames, generate random names to eliminate the attack vector with `getRandomName()` when using the `move()` method, or use the `store()` method, which automatically generates safe filenames. For text operations, if one must use ImageMagick with user-controlled text, sanitize the input to only allow safe characters and validate/restrict text options.	9.8	More Details
CVE-2025-54428	RevelaCode is an AI-powered faith-tech project that decodes biblical verses, prophecies and global events into accessible language. In versions below 1.0.1, a valid MongoDB Atlas URI with embedded username and password was accidentally committed to the public repository. This could allow unauthorized access to production or staging databases, potentially leading to data exfiltration, modification, or deletion. This is fixed in version 1.0.1. Workarounds include: immediately rotating credentials for the exposed database user, using a secret manager (like Vault, Doppler, AWS Secrets Manager, etc.) instead of storing secrets directly in code, or auditing recent access logs for suspicious activity.	9.8	More Details
CVE-2025-46059	langchain-ai v0.3.51 was discovered to contain an indirect prompt injection vulnerability in the GmailToolkit component. This vulnerability allows attackers to execute arbitrary code and compromise the application via a crafted email message.	9.8	More Details
CVE-2025-50738	The Memos application, up to version v0.24.3, allows for the embedding of markdown images with arbitrary URLs. When a user views a memo containing such an image, their browser automatically fetches the image URL without explicit user consent or interaction beyond viewing the memo. This can be exploited by an attacker to disclose the viewing user's IP address, browser User-Agent string, and potentially other request-specific information to the attacker-controlled server, leading to information disclosure and user tracking.	9.8	More Details
CVE-2025-44136	MapTiler Tileserver-php v2.0 is vulnerable to Cross Site Scripting (XSS). The GET parameter "layer" is reflected in an error message without html encoding. This leads to XSS and allows an unauthenticated attacker to execute arbitrary HTML or JavaScript code on a victim's browser.	9.8	More Details
CVE-2025-4784	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Moderec Tourtella allows SQL Injection.This issue affects Tourtella: before 26.05.2025.	9.8	More Details
CVE-2025-54438	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	9.8	More Details
CVE-2025-4822	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bayraktar Solar Energies ScadaWatt Otopilot allows SQL Injection.This issue affects ScadaWatt Otopilot: before 27.05.2025.	9.8	More Details
CVE-2025-6441	The Webinar Solution: Create live/evergreen/automated/instant webinars, stream & Zoom Meetings | WebinarIgnition plugin for WordPress is vulnerable to unauthenticated login token generation due to a missing capability check on the `webinarignition_sign_in_support_staff` and `webinarignition_register_support` functions in all versions up to, and including, 4.03.31. This makes it possible for unauthenticated attackers to generate login tokens for arbitrary WordPress users under certain circumstances, issuing authorization cookies which can lead to authentication bypass.	9.8	More Details
CVE-2025-54442	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-6380	The ONLYOFFICE Docs plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within its oo.callback REST endpoint in versions 1.1.0 to 2.2.0. The plugin's permission callback only verifies that the supplied, encrypted attachment ID maps to an existing attachment post, but does not verify the requester's identity or capabilities. This makes it possible for unauthenticated attackers to log in as an arbitrary user.	9.8	More Details
CVE-2025-54443	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	9.8	More Details
CVE-2025-54444	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-7852	The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image_upload_handle() function hooked via the 'add_new_customer' route in all versions up to, and including, 1.0.6. The plugin's image-upload handler calls move_uploaded_file() on client-supplied files without restricting allowed	9.8	More Details

	extensions or MIME types, nor sanitizing the filename. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.		
CVE-2025-7437	The Ebook Store plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ebook_store_save_form function in all versions up to, and including, 5.8012. 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-2025-54446	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	9.8	More Details
CVE-2025-54448	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-41687	An unauthenticated remote attacker may use a stack based buffer overflow in the u-link Management API to gain full access on the affected devices.	9.8	More Details
CVE-2025-54449	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-54451	Improper Control of Generation of Code ('Code Injection') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-46410	A cross-site scripting (xss) vulnerability exists in the managerPlaylists PlaylistOwnerUsersId parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	9.6	More Details
CVE-2025-50128	A cross-site scripting (xss) vulnerability exists in the videoNotFound 404ErrorMsg parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	9.6	More Details
CVE-2025-41420	A cross-site scripting (xss) vulnerability exists in the userLogin cancelUri parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	9.6	More Details
CVE-2025-30135	An issue was discovered on IROAD Dashcam FX2 devices. Dumping Files Over HTTP and RTSP Without Authentication can occur. It lacks authentication controls on its HTTP and RTSP interfaces, allowing attackers to retrieve sensitive files and video recordings. By connecting to http://192.168.10.1/mnt/extsd/event/, an attacker can download all stored video recordings in an unencrypted manner. Additionally, the RTSP stream on port 8554 is accessible without authentication, allowing an attacker to view live footage.	9.4	More Details
CVE-2025-26469	An incorrect default permissions vulnerability exists in the CServerSettings::SetRegistryValues functionality of MedDream PACS Premium 7.3.3.840. A specially crafted application can decrypt credentials stored in a configuration-related registry key. An attacker can execute a malicious script or application to exploit this vulnerability.	9.3	More Details
CVE-2025-27724	A privilege escalation vulnerability exists in the login.php functionality of meddream MedDream PACS Premium 7.3.3.840. A specially crafted .php file can lead to elevated capabilities. An attacker can upload a malicious file to trigger this vulnerability.	9.3	More Details
CVE-2025-54454	Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.1	More Details
CVE-2025-54455	Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.1	More Details
CVE-2025-53882	A Reliance on Untrusted Inputs in a Security Decision vulnerability in the logrotate configuration for openSUSEs mailman3 package allows potential escalation from mailman to root. This issue affects openSUSE Tumbleweed: from ? before 3.3.10-2.1.	9.1	More Details
CVE-2025-40599	An authenticated arbitrary file upload vulnerability exists in the SMA 100 series web management interface. A remote attacker with administrative privileges can exploit this flaw to upload arbitrary files to the system, potentially leading to remote code execution.	9.1	More Details
CVE-2025-54416	tj-actions/branch-names is a Github actions repository that contains workflows to retrieve branch or tag names with support for all events. In versions 8.2.1 and below, a critical vulnerability has been identified in the tj-actions/branch-names' GitHub Action workflow which allows arbitrary command execution in downstream workflows. This issue arises due to inconsistent input sanitization and unescaped output, enabling malicious actors to exploit specially crafted branch names or tags. While internal sanitization mechanisms have been implemented, the action outputs remain vulnerable, exposing consuming workflows to significant security risks. This is fixed in version 9.0.0	9.1	More Details
CVE-2025-8264	Versions of the package z-push/z-push-dev before 2.7.6 are vulnerable to SQL Injection due to unparameterized queries in the IMAP backend. An attacker can inject malicious commands by manipulating the username field in basic authentication. This allows the attacker to access and potentially modify or delete sensitive data from a linked third-party database. **Note:** This vulnerability affects Z-Push installations that utilize the IMAP backend and have the IMAP_FROM_SQL_QUERY option configured. Mitigation Change configuration to use the default or LDAP in backend/imap/config.php php define('IMAP_DEFAULTFROM', ''); or php define('IMAP_DEFAULTFROM', 'ldap');	9.0	More Details
CVE-2025-53084	A cross-site scripting (xss) vulnerability exists in the videosList page parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-45466	Unitree Go1 <= Go1_2022_05_11 is vulnerale to Incorrect Access Control due to authentication credentials being hardcoded in plaintext.	8.8	More Details
CVE-2025-5997	Incorrect Use of Privileged APIs vulnerability in Beamsec PhishPro allows Privilege Abuse.This issue affects PhishPro: before 7.5.4.2.	8.8	More Details
CVE-2025-41684	An authenticated remote attacker can execute arbitrary commands with root privileges on affected devices due to lack of improper sanitizing of user input in the Main Web Interface (endpoint tls_iotgen_setting).	8.8	More Details
CVE-2025-8246	A vulnerability was found in TOTOLINK X15 1.0.0-B20230714.1105. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boafrm/formRoute of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8245	A vulnerability was found in TOTOLINK X15 1.0.0-B20230714.1105. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /boafrm/formMultiAPVLAN of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8244	A vulnerability was found in TOTOLINK X15 1.0.0-B20230714.1105. It has been classified as critical. Affected is an unknown function of the file /boafrm/formMapDelDevice of the component HTTP POST Request Handler. The manipulation of the argument macstr leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8242	A vulnerability has been found in TOTOLINK X15 1.0.0-B20230714.1105 and classified as critical. This vulnerability affects unknown code of the file /boafrm/formFilter of the component HTTP POST Request Handler. The manipulation of the argument ip6addr/url/vpnPassword/vpnUser leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8184	A vulnerability was found in D-Link DIR-513 up to 1.10 and classified as critical. This issue affects the function formSetWanL2TPcallback of the file /goform/formSetWanL2TPtriggers of the component HTTP POST Request Handler. The manipulation leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-8180	A vulnerability, which was classified as critical, has been found in Tenda CH22 1.0.0.1. Affected by this issue is the function formdeleteUserName of the file /goform/deleteUserName. The manipulation of the argument old_account leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8178	A vulnerability classified as critical has been found in Tenda AC10 16.03.10.13. Affected is an unknown function of the file /goform/RequestsProcessLaid. The manipulation of the argument device1D leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8170	A vulnerability classified as critical was found in TOTOLINK T6 4.1.5cu.748_B20211015. This vulnerability affects the function tcpcheck_net of the file /router/meshSlaveDlfw of the component MQTT Packet Handler. The manipulation of the argument serverIp leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8169	A vulnerability classified as critical has been found in D-Link DIR-513 1.10. This affects the function formSetWanPPTPcallback of the file /goform/formSetWanPPTPpath of the component HTTP POST Request Handler. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-8168	A vulnerability was found in D-Link DIR-513 1.10. It has been rated as critical. Affected by this issue is the function websAspInit of the file /goform/formSetWanPPPoE. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-46198	Cross Site Scripting vulnerability in grav v.1.7.48, v.1.7.47 and v.1.7.46 allows an attacker to execute arbitrary code via the onerror attribute of the img element	8.8	More Details
CVE-2025-33076	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	8.8	More Details
CVE-2025-33077	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	8.8	More Details
CVE-2025-29629	An issue in Gardyn 4 allows a remote attacker to obtain sensitive information and execute arbitrary code via the Gardyn Home component	8.8	More Details
CVE-2025-8160	A vulnerability classified as critical has been found in Tenda AC20 up to 16.03.08.12. Affected is an unknown function of the file /goform/SetSysTimeCfg of the component httpd. The manipulation of the argument timeZone leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE-2025-8159	A vulnerability was found in D-Link DIR-513 1.0. It has been rated as critical. This issue affects the function formLanguageChange of the file /goform/formLanguageChange of the component HTTP POST Request Handler. The manipulation of the argument curTime leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-52360	A Cross-Site Scripting (XSS) vulnerability exists in the OPAC search feature of Koha Library Management System v24.05. Unsanitized input entered in the search field is reflected in the search history interface, leading to the execution of arbitrary JavaScript in the browser context when the user interacts with the interface.	8.8	More Details
CVE-2025-8140	A vulnerability was found in TOTOLINK A702R 4.0.0-B20230721.1521. It has been declared as critical. This vulnerability affects unknown code of the file /boafrm/formWlanMultipleAP of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8139	A vulnerability was found in TOTOLINK A702R 4.0.0-B20230721.1521. It has been classified as critical. This affects an unknown part of the file /boafrm/formPortFw of the component HTTP POST Request Handler. The manipulation of the argument service_type leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8138	A vulnerability was found in TOTOLINK A702R 4.0.0-B20230721.1521 and classified as critical. Affected by this issue is some unknown functionality of the file /boafrm/formOneKeyAccessButton of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8137	A vulnerability has been found in TOTOLINK A702R 4.0.0-B20230721.1521 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /boafrm/formIpQoS of the component HTTP POST Request Handler. The manipulation of the argument mac leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8136	A vulnerability, which was classified as critical, was found in TOTOLINK A702R 4.0.0-B20230721.1521. Affected is an unknown function of the file /boafrm/formFilter of the component HTTP POST Request Handler. The manipulation of the argument ip6addr leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-5835	The Droip plugin for WordPress is vulnerable to unauthorized modification and access of data due to a missing capability check on the droip_post_apis() function in all versions up to, and including, 2.2.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform many actions as the AJAX hooks to several functions. Some potential impacts include arbitrary post deletion, arbitrary post creation, post duplication, settings update, user manipulation, and much more.	8.8	More Details
CVE-2025-5831	The Droip plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the make_google_font_offline() function in all versions up to, and including, 2.2.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-8131	A vulnerability was found in Tenda AC20 16.03.08.05. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2015-10144	The Responsive Thumbnail Slider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type sanitization in the via the image uploader in versions up to 1.0.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected sites server using a double extension which may make remote code execution possible.	8.8	More Details
CVE-2025-25214	A race condition vulnerability exists in the aVideoEncoder.json.php unzip functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A series of specially crafted HTTP request can lead to arbitrary code execution.	8.8	More Details
CVE-2025-7695	The Dataverse Integration plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization checks within its reset_password_link REST endpoint in versions 2.77 through 2.81. The endpoint’s handler accepts a client-supplied id, email, or login, looks up that user, and calls get_password_reset_key() unconditionally. Because it only checks that the caller is authenticated, and not that they own or may edit the target account, any authenticated attacker, with Subscriber-level access and above, can obtain a password reset link for an administrator and hijack that account.	8.8	More Details
CVE-2025-41683	An authenticated remote attacker can execute arbitrary commands with root privileges on affected devices due to lack of improper sanitizing of user input in the Main Web Interface (endpoint event_mail_test).	8.8	More Details
CVE-2025-8243	A vulnerability was found in TOTOLINK X15 1.0.0-B20230714.1105 and classified as critical. This issue affects some unknown processing of the file /boafrm/formMapDel of the component HTTP POST Request Handler. The manipulation of the argument devicemac1 leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-42655	An access control issue in NanoMQ v0.21.10 allows attackers to bypass security restrictions and access sensitive system topic messages using MQTT wildcard characters.	8.8	More Details
CVE-2025-	Versions of the package bun after 0.0.12 are vulnerable to Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the $ shell API due to improper neutralization of user input. An attacker can exploit this by providing specially crafted input that includes command-line arguments or shell metacharacters, leading to unintended	8.8	More

8022	command execution. **Note:** This issue relates to the widely known and actively developed 'Bun' JavaScript runtime. The bun package on NPM at versions 0.0.12 and below belongs to a different and older project that happened to claim the 'bun' name in the past.		Details
CVE-2025-6190	The Realty Portal – Agent plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within the rp_user_profile() AJAX handler in versions 0.1.0 through 0.3.9. The handler reads the client-supplied meta key and value pairs from $_POST and passes them directly to update_user_meta() without restricting to a safe whitelist. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the wp_capabilities meta and grant themselves the administrator role.	8.8	More Details
CVE-2025-54453	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.8	More Details
CVE-2025-29534	An authenticated remote code execution vulnerability in PowerStick Wave Dual-Band Wifi Extender V1.0 allows an attacker with valid credentials to execute arbitrary commands with root privileges. The issue stems from insufficient sanitization of user-supplied input in the /cgi-bin/cgi_vista.cgi executable, which is passed to a system-level function call.	8.8	More Details
CVE-2025-54769	An authenticated, read-only user can upload a file and perform a directory traversal to have the uploaded file placed in a location of their choosing. This can be used to overwrite existing PERL modules within the application to achieve remote code execution (RCE) by an attacker.	8.8	More Details
CVE-2025-7722	The Social Streams plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.0.1. This is due to the plugin not properly validating a user's identity prior to updating their user meta information in the update_user_meta() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change their user type to that of an administrator.	8.8	More Details
CVE-2025-8060	A vulnerability has been found in Tenda AC23 16.03.07.52 and classified as critical. Affected by this vulnerability is the function sub_46C940 of the file /goform/setMacFilterCfg of the component httpd. The manipulation of the argument deviceList leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-54441	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.8	More Details
CVE-2025-7689	The Hydra Booking plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the tfhb_reset_password_callback() function in versions 1.1.0 to 1.1.18. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the password of an Administrator user, achieving full privilege escalation.	8.8	More Details
CVE-2025-54439	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.8	More Details
CVE-2025-4700	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that, under specific circumstances, could have potentially allowed a successful attacker to trigger unintended content rendering leading to XSS.	8.7	More Details
CVE-2025-8279	Insufficient input validation within GitLab Language Server 7.6.0 and later before 7.30.0 allows arbitrary GraphQL query execution	8.7	More Details
CVE-2025-51087	Tenda AC8V4 V16.03.34.06` was discovered to contain stack overflow at /goform/saveParentControlInfo. The manipulation of the argument time leads to stack-based buffer overflow.	8.6	More Details
CVE-2025-52452	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Salesforce Tableau Server on Windows, Linux (tabdoc api - duplicate-data-source modules) allows Absolute Path Traversal. This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.5	More Details
CVE-2025-52449	Unrestricted Upload of File with Dangerous Type vulnerability in Salesforce Tableau Server on Windows, Linux (Extensible Protocol Service modules) allows Alternative Execution Due to Deceptive Filenames (RCE). This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.5	More Details
CVE-2025-6504	In HDP Server versions below 4.6.2.2978 on Linux, unauthorized access could occur via IP spoofing using the X-Forwarded-For header. Since XFF is a client-controlled header, it could be spoofed, allowing unauthorized access if the spoofed IP matched a whitelisted range. This vulnerability could be exploited to bypass IP restrictions, though valid user credentials would still be required for resource access.	8.4	More Details
CVE-2025-36548	A cross-site scripting (xss) vulnerability exists in the LoginWordPress loginForm cancelUri parameter functionality of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get a user to visit a webpage to trigger this vulnerability.	8.3	More Details
CVE-2025-54378	HAX CMS allows you to manage your microsite universe with PHP or NodeJs backends. In versions 11.0.13 and below of haxcms-nodejs and versions 11.0.8 and below of haxcms-php, API endpoints do not perform authorization checks when interacting with a resource. Both the JS and PHP versions of the CMS do not verify that a user has permission to interact with a resource before performing a given operation. The API endpoints within the HAX CMS application check if a user is authenticated, but don't check for authorization before performing an operation. This is fixed in versions 11.0.14 of haxcms-nodejs and 11.0.9 of haxcms-php.	8.3	More Details
CVE-2025-36727	Inclusion of Functionality from Untrusted Control Sphere vulnerability in Simplehelp.This issue affects Simplehelp: before 5.5.12.	8.3	More Details

CVE-2025-52453	Server-Side Request Forgery (SSRF) vulnerability in Salesforce Tableau Server on Windows, Linux (Flow Data Source modules) allows Resource Location Spoofing. This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.2	More Details
CVE-2025-31965	Improper access restrictions in HCL BigFix Remote Control Server WebUI (versions 10.1.0.0248 and lower) allow non-admin users to view unauthorized information on certain web pages.	8.2	More Details
CVE-2025-8267	Versions of the package ssrfcheck before 1.2.0 are vulnerable to Server-Side Request Forgery (SSRF) due to an incomplete denylist of IP address ranges. Specifically, the package fails to classify the reserved IP address space 224.0.0.0/4 (Multicast) as invalid. This oversight allows attackers to craft requests targeting these multicast addresses.	8.2	More Details
CVE-2025-54445	Improper Restriction of XML External Entity Reference vulnerability in Samsung Electronics MagicINFO 9 Server allows Server Side Request Forgery.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.2	More Details
CVE-2025-8020	All versions of the package private-ip are vulnerable to Server-Side Request Forgery (SSRF) where an attacker can provide an IP or hostname that resolves to a multicast IP address (224.0.0.0/4) which is not included as part of the private IP ranges in the package's source code.	8.2	More Details
CVE-2025-44137	MapTiler Tileserver-php v2.0 is vulnerable to Directory Traversal. The renderTile function within tileserver.php is responsible for delivering tiles that are stored as files on the server via web request. Creating the path to a file allows the insertion of "../" and thus read any file on the web server. Affected GET parameters are "TileMatrix", "TileRow", "TileCol" and "Format"	8.2	More Details
CVE-2025-54447	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.1	More Details
CVE-2025-45346	SQL Injection vulnerability in Bacula-web before v.9.7.1 allows a remote attacker to execute arbitrary code via a crafted HTTP GET request.	8.1	More Details
CVE-2025-29628	An issue in Gardyn 4 allows a remote attacker to obtain sensitive information and execute arbitrary code via a request	8.1	More Details
CVE-2025-31701	A vulnerability has been found in Dahua products. Attackers could exploit a buffer overflow vulnerability by sending specially crafted malicious packets, potentially causing service disruption (e.g., crashes) or remote code execution (RCE). Some devices may have deployed protection mechanisms such as Address Space Layout Randomization (ASLR), which reduces the likelihood of successful RCE exploitation. However, denial-of-service (DoS) attacks remain a concern.	8.1	More Details
CVE-2025-6989	The Kallyas theme for WordPress is vulnerable to arbitrary folder deletion due to insufficient file path validation in the delete_font() function in all versions up to, and including, 4.21.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary folders on the server.	8.1	More Details
CVE-2025-29630	An issue in Gardyn 4 allows a remote attacker with the corresponding ssh private key can gain remote root access to affected devices	8.1	More Details
CVE-2025-31700	A vulnerability has been found in Dahua products. Attackers could exploit a buffer overflow vulnerability by sending specially crafted malicious packets, potentially causing service disruption (e.g., crashes) or remote code execution (RCE). Some devices may have deployed protection mechanisms such as Address Space Layout Randomization (ASLR), which reduces the likelihood of successful RCE exploitation. However, denial-of-service (DoS) attacks remain a concern.	8.1	More Details
CVE-2025-52448	Authorization Bypass Through User-Controlled Key vulnerability in Salesforce Tableau Server on Windows, Linux (validate-initial-sql api modules) allows Interface Manipulation (data access to the production database cluster). This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.1	More Details
CVE-2025-6505	Unauthorized access and impersonation can occur in versions 4.6.2.3226 and below of Progress Software's Hybrid Data Pipeline Server on Linux. This vulnerability allows attackers to combine credentials from different sources, potentially leading to client impersonation and unauthorized access. When OAuth Clients perform an OAuth handshake with the Hybrid Data Pipeline Server, the server accepts client credentials from both HTTP headers and request parameters.	8.1	More Details
CVE-2025-7640	The hiWeb Export Posts plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.9.0.0. This is due to missing or incorrect nonce validation on the tool-dashboard-history.php file. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php), via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.1	More Details
CVE-2025-52447	Authorization Bypass Through User-Controlled Key vulnerability in Salesforce Tableau Server on Windows, Linux (set-initial-sql tabdoc command modules) allows Interface Manipulation (data access to the production database cluster). This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.1	More Details
CVE-2025-52446	Authorization Bypass Through User-Controlled Key vulnerability in Salesforce Tableau Server on Windows, Linux (tab-doc api modules) allows Interface Manipulation (data access to the production database cluster).This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.0	More Details
CVE-2025-53078	Deserialization of Untrusted Data in Samsung DMS(Data Management Server) allows attackers to execute arbitrary code via write file to system	8.0	More Details

CVE-2025-6637	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-6636	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force a Use-After-Free vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-7497	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-7675	A maliciously crafted 3DM file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-6635	A maliciously crafted PRT file, when linked or imported into certain Autodesk products, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-6631	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-33092	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 is vulnerable to a stack-based buffer overflow in db2fm, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	7.8	More Details
CVE-2025-5043	A maliciously crafted 3DM file, when linked or imported into certain Autodesk products, can force a Heap-Based Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-5039	A maliciously crafted binary file, when present while loading files in certain Autodesk applications, could lead to execution of arbitrary code in the context of the current process due to an untrusted search path being utilized.	7.8	More Details
CVE-2025-5038	A maliciously crafted X_T file, when parsed through certain Autodesk products, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-7361	A code injection vulnerability due to an improper initialization check exists in NI LabVIEW that may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI using a CIN node. This vulnerability affects 32-bit NI LabVIEW 2025 Q1 and prior versions. LabVIEW 64-bit versions do not support CIN nodes and are not affected.	7.8	More Details
CVE-2025-7848	A memory corruption vulnerability due to improper input validation in lvpict.cpp exists in NI LabVIEW that may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q1 and prior versions.	7.8	More Details
CVE-2025-54377	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. In versions 3.23.18 and below, RooCode does not validate line breaks (\n) in its command input, allowing potential bypass of the allow-list mechanism. The project appears to lack parsing or validation logic to prevent multi-line command injection. When commands are evaluated for execution, only the first line or token may be considered, enabling attackers to smuggle additional commands in subsequent lines. This is fixed in version 3.23.19.	7.8	More Details
CVE-2025-26397	SolarWinds Observability Self-Hosted is susceptible to Deserialization of Untrusted Data Local Privilege Escalation vulnerability. An attacker with low privileges can escalate privileges to run malicious files copied to a permission-protected folder. This vulnerability requires authentication from a low-level account and local access to the host server.	7.8	More Details
CVE-2025-7849	A memory corruption vulnerability due to improper error handling when a VILinkObj is null exists in NI LabVIEW that may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q1 and prior versions.	7.8	More Details
CVE-2025-6018	A Local Privilege Escalation (LPE) vulnerability has been discovered in pam-config within Linux Pluggable Authentication Modules (PAM). This flaw allows an unprivileged local attacker (for example, a user logged in via SSH) to obtain the elevated privileges normally reserved for a physically present, "allow_active" user. The highest risk is that the attacker can then perform all allow_active yes Polkit actions, which are typically restricted to console users, potentially gaining unauthorized control over system configurations, services, or other sensitive operations.	7.8	More Details
CVE-2025-2633	Out of bounds read vulnerability due to improper bounds checking in NI LabVIEW in lvre!UDecStrToNum that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q1 and prior versions.	7.8	More Details
CVE-2025-2634	Out of bounds read vulnerability due to improper bounds checking in NI LabVIEW in fontmgr may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q1 and prior versions.	7.8	More Details
CVE-2025-8069	During the AWS Client VPN client installation on Windows devices, the install process references the C:\usr\local\windows-x86_64-openssl-localbuild\ssl directory location to fetch the OpenSSL configuration file. As a result, a non-admin user could place arbitrary code in the configuration file. If an admin user starts the AWS Client VPN client installation process, that code could be executed with root-level privileges. This issue does not affect Linux or Mac devices. We recommend users discontinue any new installations of AWS Client VPN on Windows prior to version 5.2.2.	7.8	More Details

CVE-2025-54531	In JetBrains TeamCity before 2025.07 path traversal was possible via plugin unpacking on Windows	7.7	More Details
CVE-2025-47281	Kyverno is a policy engine designed for cloud native platform engineering teams. In versions 1.14.1 and below, a Denial of Service (DoS) vulnerability exists due to improper handling of JMESPath variable substitutions. Attackers with permissions to create or update Kyverno policies can craft expressions using the {{@}} variable combined with a pipe and an invalid JMESPath function (e.g., {{@ | non_existent_function }}). This leads to a nil value being substituted into the policy structure. Subsequent processing by internal functions, specifically getValueAsStringMap, which expect string values, results in a panic due to a type assertion failure (interface {} is nil, not string). This crashes Kyverno worker threads in the admission controller and causes continuous crashes of the reports controller pod. This is fixed in version 1.14.2.	7.7	More Details
CVE-2025-51970	A SQL Injection vulnerability exists in the action.php endpoint of PuneethReddyHC Online Shopping System Advanced 1.0 due to improper sanitization of user-supplied input in the keyword POST parameter.	7.7	More Details
CVE-2025-4439	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that could have allowed an authenticated user to perform cross-site scripting attacks when the instance is served through certain content delivery networks.	7.7	More Details
CVE-2025-28170	Grandstream Networks GXP1628 <=1.0.4.130 is vulnerable to Incorrect Access Control. The device is configured with directory listing enabled, allowing unauthorized access to sensitive directories and files.	7.6	More Details
CVE-2025-31955	HCL iAutomate is affected by a sensitive data exposure vulnerability. This issue may allow unauthorized access to sensitive information within the system.	7.6	More Details
CVE-2025-40597	A Heap-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.	7.5	More Details
CVE-2025-6991	The kallyas theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.21.0 via the 'TH_LatestPosts4` widget. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	7.5	More Details
CVE-2024-13507	The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to time-based SQL Injection via the dist parameter in all versions up to, and including, 2.8.97 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-2024-49342	IBM Informix Dynamic Server 12.10 and 14.10 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.	7.5	More Details
CVE-2025-8198	The MinimogWP – The High Converting eCommerce WordPress Theme theme for WordPress is vulnerable to price manipulation in all versions up to, and including, 3.9.0. This is due to an insufficient check on quantity values when changing quantities in the cart. This makes it possible for unauthenticated attackers to add items to the cart and adjust the quantity to a fractional amount, causing the price to change based on the fractional amount. The vulnerability cannot be exploited if WooCommerce version 9.8.2+ is installed.	7.5	More Details
CVE-2025-33109	IBM i 7.2, 7.3, 7.4, 7.5, and 7.6 is vulnerable to a privilege escalation caused by an invalid database authority check. A bad actor could execute a database procedure or function without having all required permissions, in addition to causing denial of service for some database actions.	7.5	More Details
CVE-2023-7306	The Frontend File Manager Plugin plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the wpfm_delete_multiple_files() function in all versions up to, and including, 21.5. This makes it possible for unauthenticated attackers to delete arbitrary posts.	7.5	More Details
CVE-2025-50490	Improper session invalidation in the component /elms/emp-changepassword.php of PHPGurukul Student Result Management System v2.0 allows attackers to execute a session hijacking attack.	7.5	More Details
CVE-2025-50493	Improper session invalidation in the component /doctor/change-password.php of PHPGurukul Doctor Appointment Management System v1 allows attackers to execute a session hijacking attack.	7.5	More Details
CVE-2025-50494	Improper session invalidation in the component /doctor/change-password.php of PHPGurukul Car Washing Management System v1.0 allows attackers to execute a session hijacking attack.	7.5	More Details
CVE-2025-6495	The Bricks theme for WordPress is vulnerable to blind SQL Injection via the ‘p’ parameter in all versions up to, and including, 1.12.4 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-2025-53537	LibHTP is a security-aware parser for the HTTP protocol and its related bits and pieces. In versions 0.5.50 and below, there is a traffic-induced memory leak that can starve the process of memory, leading to loss of visibility. To workaround this issue, set `suricata.yaml app-layer.protocols.http.libhtp.default-config.lzma-enabled` to false. This issue is fixed in version 0.5.51.	7.5	More Details

CVE-2025-8183	NULL Pointer Dereference in µD3TN via non-singleton destination Endpoint Identifier allows remote attacker to reliably cause DoS	7.5	More Details
CVE-2025-54530	In JetBrains TeamCity before 2025.07 privilege escalation was possible due to incorrect directory permissions	7.5	More Details
CVE-2025-8021	All versions of the package files-bucket-server are vulnerable to Directory Traversal where an attacker can traverse the file system and access files outside of the intended directory.	7.5	More Details
CVE-2025-50489	Improper session invalidation in the component /srms/change-password.php of PHPGurukul Student Result Management System v2.0 allows attackers to execute a session hijacking attack.	7.5	More Details
CVE-2025-47187	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones through 6.4 SP4 (R6.4.0.4006), and the 6970 Conference Unit through 6.4 SP4 (R6.4.0.4006) or version V1 R0.1.0, could allow an unauthenticated attacker to perform a file upload attack due to missing authentication mechanisms. A successful exploit could allow an attacker to upload arbitrary WAV files, which may potentially exhaust the phone’s storage without affecting the phone's availability or operation.	7.5	More Details
CVE-2025-50492	Improper session invalidation in the component /edms/change-password.php of PHPGurukul e-Diary Management System v1 allows attackers to execute a session hijacking attack.	7.5	More Details
CVE-2024-42651	NanoMQ v0.17.9 was discovered to contain a heap use-after-free vulnerability via the component sub_Ctx_handle. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted SUBSCRIBE message.	7.5	More Details
CVE-2025-8194	There is a defect in the CPython “tarfile” module affecting the “TarFile” extraction and entry enumeration APIs. The tar implementation would process tar archives with negative offsets without error, resulting in an infinite loop and deadlock during the parsing of maliciously crafted tar archives. This vulnerability can be mitigated by including the following patch after importing the “tarfile” module: https://gist.github.com/sethmlarson/1716ac5b82b73dbcbf23ad2eff8b33e1	7.5	More Details
CVE-2025-8237	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/update_s1.php. The manipulation of the argument credits 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-2025-8270	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been classified as critical. This affects an unknown part of the file /admin/delete_s2.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8269	A vulnerability was found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/delete_s1.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8236	A vulnerability was found in code-projects Online Ordering System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/edit_product.php. The manipulation of the argument Name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-48732	An incomplete blacklist exists in the .htaccess sample of WWBN AVideo 14.4 and dev master commit 8a8954ff. A specially crafted HTTP request can lead to a arbitrary code execution. An attacker can request a .phar file to trigger this vulnerability.	7.3	More Details
CVE-2025-8173	A vulnerability has been found in 1000 Projects ABC Courier Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Add_reciver.php. The manipulation of the argument reciver_name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8166	A vulnerability was found in code-projects Church Donation System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/index.php of the component HTTP POST Request Handler. The manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8238	A vulnerability classified as critical has been found in code-projects Exam Form Submission 1.0. Affected is an unknown function of the file /admin/update_s2.php. The manipulation of the argument credits leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8271	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/delete_s3.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8274	A vulnerability classified as critical was found in Campcodes Online Recruitment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=save_recruitment_status. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8233	A vulnerability has been found in code-projects Online Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/user.php. The manipulation of the argument un leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-	An issue was discovered in Couchbase Sync Gateway before 3.2.6. In sgcollect_info_options.log and sync_gateway.log, there	7.3	More

52490	are cleartext passwords in redacted and unredacted output.		Details
CVE-2025-8232	A vulnerability, which was classified as critical, was found in code-projects Online Ordering System 1.0. Affected is an unknown function of the file /admin/delete_user.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8241	A vulnerability, which was classified as critical, was found in 1000 Projects ABC Courier Management System 1.0. This affects an unknown part of the file /report.php. The manipulation of the argument From 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-2025-8235	A vulnerability was found in code-projects Online Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/product.php. The manipulation of the argument Name 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-2025-8250	A vulnerability, which was classified as critical, was found in code-projects Exam Form Submission 1.0. Affected is an unknown function of the file /admin/update_s4.php. The manipulation of the argument credits leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8251	A vulnerability has been found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/delete_s4.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8273	A vulnerability classified as critical has been found in code-projects Exam Form Submission 1.0. Affected is an unknown function of the file /admin/update_s8.php. The manipulation of the argument credits leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-54452	Improper Authentication vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	7.3	More Details
CVE-2025-8252	A vulnerability was found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/delete_s5.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8253	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been classified as critical. This affects an unknown part of the file /admin/delete_s6.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8185	A vulnerability was found in 1000 Projects ABC Courier Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /getbyid.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8239	A vulnerability classified as critical was found in code-projects Exam Form Submission 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/. The manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8255	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been rated as critical. This issue affects some unknown processing of the file /register.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8249	A vulnerability, which was classified as critical, has been found in code-projects Exam Form Submission 1.0. This issue affects some unknown processing of the file /admin/update_s3.php. The manipulation of the argument credits 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-2025-8259	A vulnerability, which was classified as critical, was found in Vaelsys 4.1.0. This affects the function execute_DataObjectProc of the file /grid/vgrid_server.php. The manipulation of the argument xajaxargs leads to os command injection. It is possible to initiate 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.	7.3	More Details
CVE-2025-8272	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/update_fst.php. The manipulation of the argument credits 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-2025-8234	A vulnerability was found in code-projects Online Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/delete_member.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8248	A vulnerability classified as critical was found in code-projects Online Ordering System 1.0. This vulnerability affects unknown code of the file /signup.php. The manipulation of the argument firstname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-8261	A vulnerability was found in Vaelsys 4.1.0 and classified as critical. This issue affects some unknown processing of the file /grid/vgrid_server.php of the component User Creation Handler. The manipulation leads to improper authorization. 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.	7.3	More Details
CVE-2025-8179	A vulnerability classified as critical was found in PHPGurukul Local Services Search Engine Management System 2.1. Affected by this vulnerability is an unknown functionality of the file /admin/changeimage.php. The manipulation of the argument editid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-	A vulnerability classified as critical has been found in Engeman Web up to 12.0.0.1. Affected is an unknown function of the file /Login/RecoveryPass of the component Password Recovery Page. The manipulation of the argument LanguageCombobox leads	7.3	More

8220	to sql injection. 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.		Details
CVE-2025-8240	A vulnerability, which was classified as critical, has been found in code-projects Exam Form Submission 1.0. Affected by this issue is some unknown functionality of the file /user/dashboard.php. The manipulation of the argument phone 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-2025-40596	A Stack-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.	7.3	More Details
CVE-2023-53155	goform/formTest in EmbedThis GoAhead 2.5 allows HTML injection via the name parameter.	7.2	More Details
CVE-2024-53286	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in DDNS Record functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to execute arbitrary code via unspecified vectors.	7.2	More Details
CVE-2025-2928	SQL Injection affecting the Archiver role.	7.2	More Details
CVE-2025-54450	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	7.2	More Details
CVE-2025-6175	Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability in DECE Software Geodi allows HTTP Request Splitting.This issue affects Geodi: before GEODI Setup 9.0.146.	7.2	More Details
CVE-2025-54597	LinuxServer.io Heimdall before 2.7.3 allows XSS via the q parameter.	7.2	More Details
CVE-2025-8181	A vulnerability, which was classified as critical, was found in TOTOLINK N600R and X2000R 1.0.0.1. This affects an unknown part of the file vsftpd.conf of the component FTP Service. The manipulation leads to least privilege violation. It is possible to initiate the attack remotely.	7.2	More Details
CVE-2024-48729	An issue in ETSI Open-Source MANO (OSM) v.14.x, v.15.x allows a remote attacker to escalate privileges via the /osm/admin/v1/users component	7.1	More Details
CVE-2025-53080	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in Samsung DMS(Data Management Server) allows authenticated attackers to create arbitrary files in unintended locations on the filesystem	7.1	More Details
CVE-2025-31953	HCL iAutomate includes hardcoded credentials which may result in potential exposure of confidential data if intercepted or accessed by unauthorized parties.	7.1	More Details
CVE-2025-50488	Improper session invalidation in the component /library/change-password.php of PHPGurukul Online Library Management System v3.0 allows attackers to execute a session hijacking attack.	7.1	More Details
CVE-2025-50486	Improper session invalidation in the component /carrental/update-password.php of PHPGurukul Car Rental Project v3.0 allows attackers to execute a session hijacking attack.	7.1	More Details
CVE-2025-50491	Improper session invalidation in the component /banker/change-password.php of PHPGurukul Bank Locker Management System v1 allows attackers to execute a session hijacking attack.	7.1	More Details
CVE-2025-46099	In Pluck CMS 4.7.20-dev, an authenticated attacker can upload or create a crafted PHP file under the albums module directory and access it via the module routing logic in albums.site.php, resulting in arbitrary command execution through a GET parameter.	7.1	More Details
CVE-2025-31952	HCL iAutomate is affected by an insufficient session expiration. This allows tokens to remain valid indefinitely unless manually revoked, increasing the risk of unauthorized access.	7.1	More Details
CVE-2025-50484	Improper session invalidation in the component /crm/change-password.php of PHPGurukul Small CRM v3.0 allows attackers to execute a session hijacking attack.	7.1	More Details
CVE-2025-50487	Improper session invalidation in the component /bbdms/change-password.php of PHPGurukul Blood Bank & Donor Management System v2.4 allows attackers to execute a session hijacking attack.	7.1	More Details
CVE-2025-50485	Improper session invalidation in the component /crm/change-password.php of PHPGurukul Online Course Registration v3.1 allows attackers to execute a session hijacking attack.	7.1	More Details

CVE-2025-45467	Unitree Go1 <= Go1_2022_05_11 is vulnerable to Insecure Permissions as the firmware update functionality (via Wi-Fi/Ethernet) implements an insecure verification mechanism that solely relies on MD5 checksums for firmware integrity validation.	7.1	More Details
CVE-2025-4395	Medtronic MyCareLink Patient Monitor has a built-in user account with an empty password, which allows an attacker with physical access to log in with no password and access modify system functionality. This issue affects MyCareLink Patient Monitor models 24950 and 24952: before June 25, 2025	6.8	More Details
CVE-2025-4394	Medtronic MyCareLink Patient Monitor uses an unencrypted filesystem on internal storage, which allows an attacker with physical access to read and modify files. This issue affects MyCareLink Patient Monitor models 24950 and 24952: before June 25, 2025	6.8	More Details
CVE-2025-8231	A vulnerability, which was classified as critical, has been found in D-Link DIR-890L up to 111b04. This issue affects some unknown processing of the file rgbin of the component UART Port. The manipulation leads to hard-coded credentials. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.8	More Details
CVE-2024-49828	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5.0.0 through 10.5.0.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	6.5	More Details
CVE-2025-36071	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query due to improper release of memory resources.	6.5	More Details
CVE-2024-51473	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5.0.0 through 10.5.0.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	6.5	More Details
CVE-2025-44608	CloudClassroom-PHP Project v1.0 was discovered to contain a SQL injection vulnerability via the viewid parameter.	6.5	More Details
CVE-2025-6214	The Omnishop plugin for WordPress is vulnerable to Cross-Site Request Forgery on its /users/delete REST route in all versions up to, and including, 1.0.9. The route’s permission_callback only verifies that the requester is logged in, but fails to require any nonce or other proof of intent. This makes it possible for unauthenticated attackers to delete arbitrary user accounts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2025-51045	Phpgurukul Pre-School Enrollment System 1.0 contains a SQL injection vulnerability in the /admin/password-recovery.php file. This vulnerability is attributed to the insufficient validation of user input for the username parameter.	6.5	More Details
CVE-2025-51089	Tenda AC8V4 V16.03.34.06` was discovered to contain heap overflow at /goform/GetParentControlInfo.The manipulation of the argument `mac` leads to heap-based buffer overflow.	6.5	More Details
CVE-2025-28172	Grandstream Networks UCM6510 v1.0.20.52 and before is vulnerable to Improper Restriction of Excessive Authentication Attempts. An attacker can perform an arbitrary number of authentication attempts using different passwords and eventually gain access to the targeted account using a brute force attack.	6.5	More Details
CVE-2025-54380	Opencast is a free, open-source platform to support the management of educational audio and video content. Prior to version 17.6, Opencast would incorrectly send the hashed global system account credentials (ie: org.opencastproject.security.digest.user and org.opencastproject.security.digest.pass) when attempting to fetch mediapackage elements included in a mediapackage XML file. A previous CVE prevented many cases where the credentials were inappropriately sent, but not all. Anyone with ingest permissions could cause Opencast to send its hashed global system account credentials to a url of their choosing. This issue is fixed in Opencast 17.6.	6.5	More Details
CVE-2025-28171	An issue in Grandstream UCM6510 v.1.0.20.52 and before allows a remote attacker to obtain sensitive information via the Login function at /cgi and /webrtccgi.	6.5	More Details
CVE-2025-52284	Totolink X6000R V9.4.0cu.1360_B20241207 was found to contain a command injection vulnerability in the sub_4184C0 function via the tz parameter. This vulnerability allows unauthenticated attackers to execute arbitrary commands via a crafted request.	6.5	More Details
CVE-2025-36010	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 could allow an unauthenticated user to cause a denial of service due to executable segments that are waiting for each other to release a necessary lock.	6.5	More Details
CVE-2025-7780	The AI Engine plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.9.4. The simpleTranscribeAudio endpoint fails to restrict URL schemes before calling get_audio(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to read any file on the web server and exfiltrate it via the plugin’s OpenAI API integration.	6.5	More Details
CVE-2025-45731	A group deletion race condition in 2FAuth v5.5.0 causes data inconsistencies and orphaned accounts when a group is deleted while other operations are pending.	6.5	More Details
CVE-2025-51044	phpgurukul Nipah virus (NiV) Testing Management System 1.0 contains a SQL injection vulnerability in the /new-user-testing.php file, due to insufficient validation of user input for the " govtissuedid" parameter.	6.5	More Details

CVE-2025-4411	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dataprom Informatics PACS-ACSS allows Cross-Site Scripting (XSS).This issue affects PACS-ACSS: before 16.05.2025.	6.5	More Details
CVE-2025-45939	Apwide Golive 10.2.0 Jira plugin allows Server-Side Request Forgery (SSRF) via the test webhook function.	6.5	More Details
CVE-2025-5253	Allocation of Resources Without Limits or Throttling vulnerability in Kron Technologies Kron PAM allows HTTP DoS.This issue affects Kron PAM: before 3.7.	6.5	More Details
CVE-2025-4393	Medtronic MyCareLink Patient Monitor has an internal service that deserializes data, which allows a local attacker to interact with the service by crafting a binary payload to crash the service or elevate privileges. This issue affects MyCareLink Patient Monitor models 24950 and 24952: before June 25, 2025	6.5	More Details
CVE-2025-8175	A vulnerability was found in D-Link DI-8400 16.07.26A1. It has been classified as problematic. This affects an unknown part of the file usb_paswd.asp of the component jhttpd. The manipulation of the argument share_enable leads to null pointer dereference. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.5	More Details
CVE-2025-45702	SoftPerfect Pty Ltd Connection Quality Monitor v1.1 was discovered to store all credentials in plaintext.	6.5	More Details
CVE-2025-53077	An execution after redirect in Samsung DMS(Data Management Server) allows attackers to execute limited functions without permissions. An attacker could compromise the integrity of the platform by executing this vulnerability.	6.5	More Details
CVE-2025-54767	An authenticated, read-only user can kill any processes running on the Xormon Original virtual appliance as the lpar2rrd user.	6.5	More Details
CVE-2024-48730	An issue in ETSI Open-Source MANO (OSM) v.14.x, v.15.x allows a remote attacker to escalate privileges via not imposing any restrictions on the authentication attempts performed by an admin user	6.5	More Details
CVE-2025-6539	The Voltax Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.6.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7501	The Wonder Slider Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image title and description DOM in all versions up to, and including, 14.4 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-2025-7809	The StreamWeasels Twitch Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'data-uuid' attribute in all versions up to, and including, 1.9.3 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-2025-7811	The StreamWeasels YouTube Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'data-uuid' attribute in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-3075	The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'elementor-element' shortcode in all versions up to, and including, 3.29.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only impacts sites with 'Element Caching' enabled.	6.4	More Details
CVE-2025-4566	The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the data-text DOM element attribute in Text Path widget in all versions up to, and including, 3.30.2 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. This attack affects only Chrome/Edge browsers	6.4	More Details
CVE-2025-4968	The WPBakery Page Builder for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple Page Builder elements (Copyright Element, Hover Box, Separator With Text, FAQ, Single Image, Custom Header, Button, Call To Action, Progress Bar, Pie Chart, Round Chart, and Line Chart) in all versions up to, and including, 8.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-5529	The Educenter theme for WordPress is vulnerable to Stored Cross-Site Scripting via the Circle Counter Block in all versions up to, and including, 1.6.2 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-	Zohocorp ManageEngine Applications Manager versions 176600 and prior are vulnerable to stored cross-site scripting in the File/Directory monitor.	6.4	More Details

27930			
CVE-2025-6387	The WP Get The Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8196	The Magical Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Attributes in all versions up to, and including, 1.3.8 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-2025-6385	The WP Applink plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title’ parameter in all versions up to, and including, 0.4.1 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-2025-53081	An 'Arbitrary File Creation' in Samsung DMS(Data Management Server) allows attackers to create arbitrary files in unintended locations on the filesystem. Exploitation is restricted to specific, authorized private IP addresses.	6.4	More Details
CVE-2025-6382	The Taeggie Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's taeggie-feed shortcode in all versions up to, and including, 0.1.10. The plugin’s render() method takes the user-supplied name attribute and injects it directly into a <script> tag - both in the id attribute and inside jQuery.getScript() - without proper 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-2025-6262	The muse.ai video embedding plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's muse-ai shortcode in all versions up to, and including, 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-2025-4608	The Structured Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sc_fs_local_business shortcode in all versions up to, and including, 1.6.4 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-2025-3669	The Supreme Addons for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's auto_qrcodesabb shortcode in all versions up to, and including, 1.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6681	The Fan Page plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘width’ parameter in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6692	The YouTube Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘instance’ parameter in all versions up to, and including, 10.3 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-2025-5587	The Appzend theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘progressbarLayout’ parameter in all versions up to, and including, 1.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8216	The Sky Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Multiple widgets in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7959	The Station Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘width' and 'height’ parameter in all versions up to, and including, 2.4.2 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-2025-7966	The Get Youtube Subs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘channel', 'layout', and 'subs_count’ parameters in all versions up to, and including, 3.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-43018	Piwigo 13.8.0 and below is vulnerable to SQL Injection in the parameters max_level and min_register. These parameters are used in ws_user_gerList function from file include\ws_functions\pwg.users.php and this same function is called by ws.php file at some point can be used for searching users in advanced way in /admin.php?page=user_list.	6.4	More Details
CVE-2025-5753	The Valuation Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘link’ parameter in all versions up to, and including, 1.3.2 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-	The Fleetwire Fleet Management plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's fleetwire_list		

2025-6261	shortcode in all versions up to, and including, 1.0.19 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-2025-5684	The MetForm – Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `mf-template` DOM Element 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 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-2025-3614	The ElementsKit Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL attribute of a custom widget in all versions up to, and including, 3.5.2 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-2025-6987	The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'advanced_iframe' shortcode in all versions up to, and including, 2025.5 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-2025-8071	Mine CloudVod plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘audio’ parameter in all versions up to, and including, 2.1.10 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-2025-8219	A vulnerability was found in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.4.7. It has been rated as critical. This issue affects some unknown processing of the file /crm/crmapi/erp/tabdetail_moduleSave_dxkp.php of the component HTTP POST Request Handler. The manipulation of the argument getvaluestring leads to sql injection. The attack may be initiated remotely. Upgrading to version 8.6.5.2 is able to address this issue. It is recommended to upgrade the affected component. The vendor explains: "All SQL injection vectors were patched via parameterized queries and input sanitization in v8.6.5+. We strongly advise all customers to upgrade to the current version (v8.6.5.2), which includes this fix and additional security enhancements."	6.3	More Details
CVE-2025-8162	A vulnerability, which was classified as critical, has been found in deerwms deer-wms-2 up to 3.3. Affected by this issue is some unknown functionality of the file /system/dept/list. The manipulation of the argument params[dataScope] leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8189	A vulnerability classified as critical was found in Campcodes Courier Management System 1.0. This vulnerability affects unknown code of the file /edit_user.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8161	A vulnerability classified as critical was found in deerwms deer-wms-2 up to 3.3. Affected by this vulnerability is an unknown functionality of the file /system/role/export. The manipulation of the argument params[dataScope] leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8135	A vulnerability, which was classified as critical, has been found in itsourcecode Insurance Management System 1.0. This issue affects some unknown processing of the file /updateAgent.php. The manipulation of the argument agent_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8134	A vulnerability classified as critical was found in PHPGurukul BP Monitoring Management System 1.0. This vulnerability affects unknown code of the file /bwdates-report-result.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8158	A vulnerability was found in PHPGurukul Login and User Management System 3.3. It has been declared as critical. This vulnerability affects unknown code of the file /admin/yesterday-reg-users.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8133	A vulnerability classified as critical has been found in yanyutao0402 ChanCMS up to 3.1.2. This affects the function getArticle of the file app/modules/api/service/gather.js. The manipulation of the argument targetUrl leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. The identifier of the patch is 3ef58a50e8b3c427b03c8cf3c9e19a79aa809be6. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-8163	A vulnerability, which was classified as critical, was found in deerwms deer-wms-2 up to 3.3. This affects an unknown part of the file /system/role/list. The manipulation of the argument params[dataScope] leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8164	A vulnerability has been found in code-projects Public Chat Room 1.0 and classified as critical. This vulnerability affects unknown code of the file send_message.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8123	A vulnerability was found in deerwms deer-wms-2 up to 3.3. It has been classified as critical. Affected is an unknown function of the file /system/dept/edit. The manipulation of the argument ancestors leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8128	A vulnerability, which was classified as critical, has been found in zhousg letao up to 7d8df0386a65228476290949e0413de48f7fbe98. This issue affects some unknown processing of the file routes\bf\product.js. The manipulation of the argument pictrdtz leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may 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.	6.3	More Details
CVE-2025-	A vulnerability classified as critical was found in deerwms deer-wms-2 up to 3.3. This vulnerability affects unknown code of the file /system/user/list. The manipulation of the argument params[dataScope] leads to sql injection. The attack can be initiated	6.3	More Details

8127	remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-8230	A vulnerability classified as critical was found in Campcodes Courier Management System 1.0. This vulnerability affects unknown code of the file /manage_user.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8126	A vulnerability classified as critical has been found in deerwms deer-wms-2 up to 3.3. This affects an unknown part of the file /system/user/export. The manipulation of the argument params[dataScope] leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8172	A vulnerability, which was classified as critical, was found in itsourcecode Employee Management System 1.0. Affected is an unknown function of the file /admin/index.php. The manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8171	A vulnerability, which was classified as critical, has been found in code-projects Document Management System 1.0. This issue affects some unknown processing of the file /insert.php. The manipulation of the argument uploaded_file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8125	A vulnerability was found in deerwms deer-wms-2 up to 3.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /system/role/authUser/allocatedList. The manipulation of the argument params[dataScope] leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8190	A vulnerability, which was classified as critical, has been found in Campcodes Courier Management System 1.0. This issue affects some unknown processing of the file /print_pdets.php. The manipulation of the argument ids leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8203	A vulnerability classified as critical has been found in Jingmen Zeyou Large File Upload Control up to 6.3. Affected is an unknown function of the file /index.jsp. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-8165	A vulnerability was found in code-projects Food Review System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/approve_reservation.php. The manipulation of the argument occasion leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8247	A vulnerability classified as critical has been found in Projectworlds Online Admission System 1.0. This affects an unknown part of the file /admin.php. The manipulation of the argument markof leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8174	A vulnerability was found in code-projects Voting System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/candidates_add.php. The manipulation of the argument photo leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8188	A vulnerability classified as critical has been found in Campcodes Courier Management System 1.0. This affects an unknown part of the file /edit_staff.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8229	A vulnerability classified as critical has been found in Campcodes Courier Management System 1.0. This affects an unknown part of the file /parcel_list.php. The manipulation of the argument s leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-36728	Cross-Site Request Forgery (CSRF) vulnerability in Simplehelp.This issue affects Simplehelp: before 5.5.11.	6.3	More Details
CVE-2025-8227	A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /collect/getArticle. The manipulation of the argument taskUrl leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. The patch is named 33d9bb464353015aaaba84e27638ac9a3912795d. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-52358	A cross-site scripting vulnerability in Vivaldi United Group iCONTROL+ Server including Firmware version 4.7.8.0.eden Logic version 5.32 and below. This issue allows attackers to inject JavaScript payloads within the error or edit-menu-item parameters which are then executed in the victim's browser session.	6.3	More Details
CVE-2025-8256	A vulnerability classified as critical has been found in code-projects Online Ordering System 1.0. Affected is an unknown function of the file /admin/product.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8228	A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been rated as critical. Affected by this issue is the function getPages of the file /cms/collect/getPages. The manipulation of the argument targetUrl leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-36117	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 does not disallow the session id after use which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2025-36116	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 GUI is affected by cross-site WebSocket hijacking vulnerability. By sending a specially crafted request, an unauthenticated malicious actor could exploit this vulnerability to sniff an existing WebSocket connection to then remotely perform operations that the user is not allowed to perform.	6.3	More Details

CVE-2025-8254	A vulnerability was found in Campcodes Courier Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /view_parcel.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-54090	A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Users are recommended to upgrade to version 2.4.65, which fixes the issue.	6.3	More Details
CVE-2025-8124	A vulnerability was found in deerwms deer-wms-2 up to 3.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /system/role/authUser/unallocatedList. The manipulation of the argument params[dataScope] leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8156	A vulnerability was found in PHPGurukul User Registration & Login and User Management 3.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/lastsevendays-reg-users.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8157	A vulnerability was found in PHPGurukul User Registration & Login and User Management 3.3. It has been classified as critical. This affects an unknown part of the file /admin/lastthirtyays-reg-users.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8107	In OceanBase's Oracle tenant mode, a malicious user with specific privileges can achieve privilege escalation to SYS-level access by executing carefully crafted commands. This vulnerability only affects OceanBase tenants in Oracle mode. Tenants in MySQL mode are unaffected.	6.3	More Details
CVE-2025-8266	A vulnerability has been found in yanyutao0402 ChanCMS up to 3.1.2 and classified as critical. Affected by this vulnerability is the function getArticle of the file app/modules/cms/controller/collect.js. The manipulation of the argument targetUrl leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-8186	A vulnerability was found in Campcodes Courier Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edit_branch.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8187	A vulnerability was found in Campcodes Courier Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /edit_parcel.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-40682	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local user to cause a denial of service due to improper validation of specified type of input.	6.2	More Details
CVE-2025-33013	IBM MQ Operator LTS 2.0.0 through 2.0.29, MQ Operator CD 3.0.0, 3.0.1, 3.1.0 through 3.1.3, 3.3.0, 3.4.0, 3.4.1, 3.5.0, 3.5.1, 3.6.0, and MQ Operator SC2 3.2.0 through 3.2.13 Container could disclose sensitive information to a local user due to improper clearing of heap memory before release.	6.2	More Details
CVE-2025-45406	A stored cross-site scripting (XSS) vulnerability in CodeIgniter4 v4.6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the debugbar_time parameter. NOTE: this is disputed by the Supplier because attackers cannot influence the value of debugbar_time, and because debugbar-related data is automatically escaped by the CodeIgniter Parser class.	6.1	More Details
CVE-2025-54527	In JetBrains YouTrack before 2025.2.86935, 2025.2.87167, 2025.3.87341, 2025.3.87344 improper iframe configuration in widget sandbox allows popups to bypass security restrictions	6.1	More Details
CVE-2025-40598	A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.	6.1	More Details
CVE-2025-32731	A reflected cross-site scripting (xss) vulnerability exists in the radiationDoseReport.php functionality of meddream MedDream PACS Premium 7.3.5.860. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	6.1	More Details
CVE-2025-45892	OpenCart version 4.1.0.4 is vulnerable to a Stored Cross-Site Scripting (XSS) attack via the blog editor. The vulnerability arises because input in the blog's editor is not properly sanitized or escaped before being rendered. This allows attackers to inject malicious JavaScript code	6.1	More Details
CVE-2025-6174	The Qwizcards | online quizzes and flashcards WordPress plugin through 3.9.4 does not sanitise and escape the "_stylesheet" 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 or any other user.	6.1	More Details
CVE-2025-45893	OpenCart version 4.1.0.4 is vulnerable to a Stored Cross-Site Scripting (XSS) attack via SVG file uploads used in blog posts. The vulnerability arises because SVG files uploaded through the media manager are not properly sanitized. Attackers can craft a malicious SVG file containing embedded JavaScript	6.1	More Details
CVE-2025-45960	Cross Site Scripting vulnerability in tawk.to Live Chat v.1.6.1 allows a remote attacker to execute arbitrary code via the web application stores and displays user-supplied input without proper input validation or encoding	6.1	More Details
CVE-2025-53082	An 'Arbitrary File Deletion' in Samsung DMS(Data Management Server) allows attackers to delete arbitrary files from unintended locations on the filesystem. Exploitation is restricted to specific, authorized private IP addresses.	6.1	More Details

CVE-2025-51411	A reflected cross-site scripting (XSS) vulnerability exists in Institute-of-Current-Students v1.0 via the email parameter in the /postquerypublic endpoint. The application fails to properly sanitize user input before reflecting it in the HTML response. This allows unauthenticated attackers to inject and execute arbitrary JavaScript code in the context of the victim's browser by tricking them into visiting a crafted URL or submitting a malicious form. Successful exploitation may lead to session hijacking, credential theft, or other client-side attacks.	6.1	More Details
CVE-2025-7022	The My Reservation System WordPress plugin through 2.3 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.	6.1	More Details
CVE-2025-5254	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kron Technologies Kron PAM allows Stored XSS.This issue affects Kron PAM: before 3.7.	6.1	More Details
CVE-2025-7690	The Affiliate Plus plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.2. This is due to missing or incorrect nonce validation on the 'affiplus_settings' page. This makes it possible for unauthenticated attackers to perform an unauthorized action granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-6588	The FunnelCockpit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘error’ parameter in all versions up to, and including, 1.4.2 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 an administrative user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-5084	The Post Grid Master plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘argsArray['read_more_text']’ parameter in all versions up to, and including, 3.4.13 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-2025-6054	The YANewsflash 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 or incorrect nonce validation on the 'yanewsflash/yanewsflash.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-36005	IBM MQ Operator LTS 2.0.0 through 2.0.29, MQ Operator CD 3.0.0, 3.0.1, 3.1.0 through 3.1.3, 3.3.0, 3.4.0, 3.4.1, 3.5.0, 3.5.1, 3.6.0, and MQ Operator SC2 3.2.0 through 3.2.13 Internet Pass-Thru could allow a malicious user to obtain sensitive information from another TLS session connection by the proxy to the same hostname and port due to improper certificate validation.	5.9	More Details
CVE-2022-50237	The ed25519-dalek crate before 2 for Rust allows a double public key signing function oracle attack. The Keypair implementation leads to a simple computation for extracting a private key.	5.9	More Details
CVE-2024-53288	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in NTP Region functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to inject arbitrary web script or HTML via unspecified vectors.	5.9	More Details
CVE-2025-33020	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 transmits sensitive information without encryption that could allow an attacker to obtain highly sensitive information.	5.9	More Details
CVE-2024-53287	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in VPN Setting functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to inject arbitrary web script or HTML via unspecified vectors.	5.9	More Details
CVE-2025-7745	Buffer Over-read vulnerability in ABB AC500 V2.This issue affects AC500 V2: through 2.5.2.	5.8	More Details
CVE-2025-24485	A server-side request forgery vulnerability exists in the cecho.php functionality of MedDream PACS Premium 7.3.5.860. A specially crafted HTTP request can lead to SSRF. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	5.8	More Details
CVE-2025-54535	In JetBrains TeamCity before 2025.07 password reset and email verification tokens were using weak hashing algorithms	5.8	More Details
CVE-2025-8182	A vulnerability has been found in Tenda AC18 15.03.05.19 and classified as problematic. This vulnerability affects unknown code of the file /etc_ro/smb.conf of the component Samba. The manipulation leads to weak password requirements. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.	5.6	More Details
CVE-2025-5818	The Featured Image Plus – Quick & Bulk Edit with Unsplash plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.6.4 via the fip_get_image_options() function. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	5.5	More Details
CVE-2024-41751	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local, authenticated attacker to bypass client-side enforcement of security to manipulate data.	5.5	More Details
CVE-2025-	A global buffer overflow vulnerability was found in the soup_header_name_to_string function in Libsoup. The \`soup_header_name_to_string\` function does not validate the \`name\` parameter passed in, and directly accesses \`soup_header_name_strings[name]\`. The value of \`name\` is controllable, when \`name\` exceeds the index range of	5.5	More Details

8197	`soup_headr_name_string`, it will cause an out-of-bounds access.		
CVE-2024-41750	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local, authenticated attacker to bypass client-side enforcement of security to manipulate data.	5.5	More Details
CVE-2025-54537	In JetBrains TeamCity before 2025.07 user credentials were stored in plain text in memory snapshots	5.5	More Details
CVE-2025-42947	SAP FICA ODN framework allows a high privileged user to inject value inside the local variable which can then be executed by the application. An attacker could thereby control the behaviour of the application causing high impact on integrity, low impact on availability and no impact on confidentiality of the application.	5.5	More Details
CVE-2025-54538	In JetBrains TeamCity before 2025.07 password exposure was possible via command line in the "hg pull" command	5.5	More Details
CVE-2025-50477	A URL redirection in lbry-desktop v0.53.9 allows attackers to redirect victim users to attacker-controlled pages.	5.4	More Details
CVE-2025-44109	A URL redirection in Pinokio v3.6.23 allows attackers to redirect victim users to attacker-controlled pages.	5.4	More Details
CVE-2025-54536	In JetBrains TeamCity before 2025.07 a CSRF was possible on GraphQL endpoint	5.4	More Details
CVE-2025-46996	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-8132	A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been rated as critical. Affected by this issue is the function delfile of the file app/extend/utils.js. The manipulation leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. The name of the patch is c8a282bf02a62b59ec60b4699e91c51aff2ee9cd. It is recommended to upgrade the affected component.	5.4	More Details
CVE-2025-6060	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in DECE Software Geodi allows Cross-Site Scripting (XSS).This issue affects Geodi: before GEODI Setup 9.0.146.	5.4	More Details
CVE-2024-49343	IBM Informix Dynamic Server 12.10 and 14.10 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	5.4	More Details
CVE-2025-54528	In JetBrains TeamCity before 2025.07 a CSRF was possible in GitHub App connection flow	5.4	More Details
CVE-2025-46993	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-54423	copyparty is a portable file server. In versions up to and including versions 1.18.4, an unauthenticated attacker is able to execute arbitrary JavaScript code in a victim's browser due to improper sanitization of multimedia tags in music files, including m3u files. This is fixed in version 1.18.5.	5.4	More Details
CVE-2024-40686	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	5.4	More Details
CVE-2025-47061	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-46171	vBulletin 3.8.7 is vulnerable to a denial-of-service condition via the misc.php?do=buddylist endpoint. If an authenticated user has a sufficiently large buddy list, processing the list can consume excessive memory, exhausting system resources and crashing the forum.	5.4	More Details
CVE-2025-7810	The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'data-uuid' attribute in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-53541	Tuleap is an Open Source Suite created to facilitate management of software development and collaboration. In Tuleap Community Edition prior to version 16.9.99.1751892857 and Tuleap Enterprise Edition prior to 16.8-5 and 16.9-3, malicious users with some control over certain artifacts could insert malicious code when displaying the children of a parent artifact to force victims to execute the uncontrolled code. This is fixed in version Tuleap Community Edition prior to version 16.9.99.1751892857 and Tuleap Enterprise Edition prior to 16.8-5 and 16.9-3.	5.4	More Details

CVE-2025-54768	An API endpoint that should be limited to web application administrators is hidden from, but accessible by, lower-level read only web application users. The endpoint can be used to download logs from the appliance configuration, exposing sensitive information.	5.3	More Details
CVE-2025-52899	Tuleap is an Open Source Suite created to facilitate management of software development and collaboration. In Tuleap Community Edition prior to version 16.9.99.1750843170 and Tuleap Enterprise Edition prior to 16.8-4 and 16.9-2, the forgot password form allows for user enumeration. This is fixed in Tuleap Community Edition version 16.9.99.1750843170 and Tuleap Enterprise Edition 16.8-4 and 16.9-2.	5.3	More Details
CVE-2025-52455	Server-Side Request Forgery (SSRF) vulnerability in Salesforce Tableau Server on Windows, Linux (EPS Server modules) allows Resource Location Spoofing. This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	5.3	More Details
CVE-2025-52454	Server-Side Request Forgery (SSRF) vulnerability in Salesforce Tableau Server on Windows, Linux (Amazon S3 Connector modules) allows Resource Location Spoofing. This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	5.3	More Details
CVE-2025-8275	A vulnerability, which was classified as problematic, has been found in bsc Peru Cocktails App 1.0.0 on Android. Affected by this issue is some unknown functionality of the file AndroidManifest.xml of the component bsc.devy.peru_cocktails. The manipulation leads to improper export of android application components. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2023-53157	The rosenpass crate before 0.2.1 for Rust allows remote attackers to cause a denial of service (panic) via a one-byte UDP packet.	5.3	More Details
CVE-2025-6215	The Omnishop plugin for WordPress is vulnerable to Unauthenticated Registration Bypass in all versions up to, and including, 1.0.9. Its /users/register endpoint is exposed to the public (permission_callback always returns true) and invokes wp_create_user() unconditionally, ignoring the site’s users_can_register option and any nonce or CAPTCHA checks. This makes it possible for unauthenticated attackers to create arbitrary user accounts (customer) on sites where registrations should be closed.	5.3	More Details
CVE-2025-51085	Tenda AC8V4 V16.03.34.06` was discovered to contain stack overflow at /goform/SetSysTimeCfg. The manipulation of the argument `timeZone` and `timeType` leads to stack-based buffer overflow.	5.3	More Details
CVE-2025-2533	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	5.3	More Details
CVE-2025-4370	The Brizy – Page Builder plugin for WordPress is vulnerable to limited file uploads due to missing authorization on process_external_asset_urls function as well as missing path validation in store_file function in all versions up to, and including, 2.6.20. This makes it possible for unauthenticated attackers to upload .TXT files on the affected site's server.	5.3	More Details
CVE-2025-51088	Tenda AC8V4 V16.03.34.06` was discovered to contain stack overflow at /goform/WifiGuestSet. The manipulation of the argument `shareSpeed` leads to stack-based buffer overflow.	5.3	More Details
CVE-2025-8257	A vulnerability classified as problematic was found in Lobby Universe Lobby App up to 2.8.0 on Android. Affected by this vulnerability is an unknown functionality of the file AndroidManifest.xml of the component com.maverick.lobby. The manipulation leads to improper export of android application components. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2025-8176	A vulnerability was found in LibTIFF up to 4.7.0. It has been declared as critical. This vulnerability affects the function get_histogram of the file tools/tiffmedian.c. The manipulation leads to use after free. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The patch is identified as fe10872e53efba9cc36c66ac4ab3b41a839d5172. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-8177	A vulnerability was found in LibTIFF up to 4.7.0. It has been rated as critical. This issue affects the function setrow of the file tools/thumbnail.c. The manipulation leads to buffer overflow. An attack has to be approached locally. The patch is named e8c9d6c616b19438695fd829e58ae4fde5bfbc22. It is recommended to apply a patch to fix this issue. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2025-33114	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2 is vulnerable to denial of service with a specially crafted query under certain non-default conditions.	5.3	More Details
CVE-2025-51082	Tenda AC8V4 V16.03.34.06` was discovered to contain stack overflow at /goform/fast_setting_wifi_set. The manipulation of the argument `timeZone` leads to stack-based buffer overflow.	5.3	More Details
CVE-2025-8097	The WoodMart theme for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 8.2.6. This is due to insufficient validation of the qty parameter in the woodmart_update_cart_item function. This makes it possible for unauthenticated attackers to manipulate cart quantities using fractional values, allowing them to obtain products for free by setting extremely small quantities (e.g., 0.00001) that round cart totals to $0.00, effectively bypassing payment requirements and allowing unauthorized acquisition of virtual or downloadable products.	5.3	More Details
CVE-2025-8258	A vulnerability, which was classified as problematic, has been found in Cool Mo Maigcal Number App up to 1.0.3 on Android. Affected by this issue is some unknown functionality of the file AndroidManifest.xml of the component com.sdmagic.number. The manipulation leads to improper export of android application components. An attack has to be approached locally. The exploit has been disclosed to the public and may be used.	5.3	More Details

CVE-2025-26400	SolarWinds Web Help Desk was reported to be affected by an XML External Entity Injection (XXE) vulnerability that could lead to information disclosure. A valid, low-privilege access is required unless the attacker had access to the local server to modify configuration files.	5.3	More Details
CVE-2025-8207	A vulnerability was found in Canara ai1 Mobile Banking App 3.6.23 on Android and classified as problematic. This issue affects some unknown processing of the file AndroidManifest.xml of the component com.canarabank.mobility. The manipulation leads to improper export of android application components. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-54765	An API endpoint that should be limited to web application administrators is hidden from, but accessible by, lower-level read only web application users. The endpoint can be used to import the appliance configuration, allowing an attacker to control the configuration of the appliance, to include granting themselves administrative level permissions.	5.3	More Details
CVE-2025-54766	An API endpoint that should be limited to web application administrators is hidden from, but accessible by, lower-level read only web application users. The endpoint can be used to export the appliance configuration, exposing sensitive information.	5.3	More Details
CVE-2025-8210	A vulnerability was found in Yeelink Yeelight App up to 3.5.4 on Android. It has been classified as problematic. Affected is an unknown function of the file AndroidManifest.xml of the component com.yeelight.cherry. The manipulation leads to improper export of android application components. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-8009	The Security Ninja – WordPress Security Plugin & Firewall plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 5.242 via the 'get_file_source' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to extract sensitive data, including the contents of any file on the server.	4.9	More Details
CVE-2025-53079	Absolute Path Traversal in Samsung DMS(Data Management Server) allows authenticated attacker (Administrator) to read sensitive files	4.9	More Details
CVE-2025-30086	CNCF Harbor 2.13.x before 2.13.1 and 2.12.x before 2.12.4 allows information disclosure by administrators who can exploit an ORM Leak present in the /api/v2.0/users endpoint to leak users' password hash and salt values. The q URL parameter allows a user to filter users by any column, and filter password=~ could be abused to leak out a user's password hash character by character. An attacker with administrator access could exploit this to leak highly sensitive information stored in the Harbor database. All endpoints that support the q URL parameter are vulnerable to this ORM leak attack.	4.9	More Details
CVE-2024-52894	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5.0.0 through 10.5.0.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.2 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	4.9	More Details
CVE-2025-50481	A cross-site scripting (XSS) vulnerability in the component /blog/blogpost/add of Mezzanine CMS v6.1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into a blog post.	4.8	More Details
CVE-2025-54534	In JetBrains TeamCity before 2025.07 reflected XSS was possible on the agentpushPreset page	4.8	More Details
CVE-2025-27800	The Episerver Content Management System (CMS) by Optimizely was affected by multiple Stored Cross-Site Scripting (XSS) vulnerabilities. This allowed an authenticated attacker to execute malicious JavaScript code in the victim's browser. The Admin dashboard offered the functionality to add gadgets to the dashboard. This included the "Notes" gadget. An authenticated attacker with the corresponding access rights (such as "WebAdmin") that was impersonating the victim could insert malicious JavaScript code in these notes that would be executed if the victim visited the dashboard. Affected products: Version 11.X: EPiServer.CMS.Core (<11.21.4) with EPiServer.CMS.UI (<11.37.5), Version 12.X: EPiServer.CMS.Core (<12.22.1) with EPiServer.CMS.UI (<11.37.3)	4.8	More Details
CVE-2025-27802	The Episerver Content Management System (CMS) by Optimizely was affected by multiple Stored Cross-Site Scripting (XSS) vulnerabilities. This allowed an authenticated attacker to execute malicious JavaScript code in the victim's browser. RTE properties (text fields), which could be used in the "Edit" section of the CMS, allowed the input of arbitrary text. It was possible to input malicious JavaScript code in these properties that would be executed if a user visits the previewed page. Attackers needed at least the role "WebEditor" in order to exploit this issue. Affected products: Version 11.X: EPiServer.CMS.Core (<11.21.4) with EPiServer.CMS.UI (<11.37.5), Version 12.X: EPiServer.CMS.Core (<12.22.1) with EPiServer.CMS.UI (<11.37.3)	4.8	More Details
CVE-2025-27801	The Episerver Content Management System (CMS) by Optimizely was affected by multiple Stored Cross-Site Scripting (XSS) vulnerabilities. This allowed an authenticated attacker to execute malicious JavaScript code in the victim's browser. ContentReference properties, which could be used in the "Edit" section of the CMS, offered an upload functionality for documents. These documents could later be used as displayed content on the page. It was possible to upload SVG files that include malicious JavaScript code that would be executed if a user visited the direct URL of the preview image. Attackers needed at least the role "WebEditor" in order to exploit this issue. Affected products: Version 11.X: EPiServer.CMS.Core (<11.21.4) with EPiServer.CMS.UI (<11.37.5), Version 12.X: EPiServer.CMS.Core (<12.22.1) with EPiServer.CMS.UI (<11.37.3)	4.8	More Details
CVE-2025-8265	A vulnerability classified as critical has been found in 299Ko CMS 2.0.0. This affects an unknown part of the file /admin/filemanager/view of the component File Management. The manipulation leads to unrestricted upload. It is possible to initiate 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.	4.7	More Details
CVE-2025-4296	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in HotelRunner B2B allows Forceful Browsing.This issue affects B2B: before 04.06.2025.	4.7	More Details
CVE-2025-	A flaw was found in libssh, a library that implements the SSH protocol. When calculating the session ID during the key exchange (KEX) process, an allocation failure in cryptographic functions may lead to a NULL pointer dereference. This issue can cause the	4.7	More

8114	client or server to crash.		Details
CVE-2025-54569	In Malwarebytes Binisoft Windows Firewall Control before 6.16.0.0, the installer is vulnerable to local privilege escalation.	4.5	More Details
CVE-2023-53159	The openssl crate before 0.10.55 for Rust allows an out-of-bounds read via an empty string to X509VerifyParamRef::set_host.	4.5	More Details
CVE-2025-27514	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. In versions 9.5.0 through 10.0.18, a technician can use a malicious payload to trigger a stored XSS on the project's kanban. This is fixed in version 10.0.19.	4.5	More Details
CVE-2023-53156	The transpose crate before 0.2.3 for Rust allows an integer overflow via input_width and input_height arguments.	4.5	More Details
CVE-2025-41241	VMware vCenter contains a denial-of-service vulnerability. A malicious actor who is authenticated through vCenter and has permission to perform API calls for guest OS customisation may trigger this vulnerability to create a denial-of-service condition.	4.4	More Details
CVE-2025-7835	The iThoughts Advanced Code Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.10. This is due to missing or incorrect nonce validation on the 'ithoughts_ace_update_options' AJAX action. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-8221	A vulnerability classified as problematic was found in jerryshensjf JPACookieShop 蛋糕商城JPA版 up to 24a15c02b4f75042c9f7f615a3fed2ec1cefb999. Affected by this vulnerability is the function goodsSearch of the file GoodsCustController.java. The manipulation of the argument keyword leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may 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.	4.3	More Details
CVE-2025-7822	The WP Wallcreeper plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the admin_notices hook in all versions up to, and including, 1.6.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to enable and disable caching.	4.3	More Details
CVE-2025-8104	The Memory Usage plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.98. This is due to missing nonce validation in the wpmemory_install_plugin() function. This makes it possible for unauthenticated attackers to silently install one of the several whitelisted plugins 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-2025-8223	A vulnerability, which was classified as problematic, was found in jerryshensjf JPACookieShop 蛋糕商城JPA版 up to 24a15c02b4f75042c9f7f615a3fed2ec1cefb999. This affects an unknown part of the file AdminTypeCustController.java. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	4.3	More Details
CVE-2025-8103	The WPeMatico RSS Feed Fetcher plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.7. This is due to missing nonce validation in the handle_feedback_submission() function. This makes it possible for unauthenticated attackers to deactivate the plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-8262	A vulnerability was found in yarnpkg Yarn up to 1.22.22. It has been classified as problematic. Affected is the function explodeHostedGitFragment of the file src/resolvers/exotics/hosted-git-resolver.js. The manipulation leads to inefficient regular expression complexity. It is possible to launch the attack remotely. The patch is identified as 97731871e674bf93bcbf29e9d3258da8685f3076. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2025-53902	Tuleap is an Open Source Suite created to facilitate management of software development and collaboration. In Tuleap Community Edition prior to version 16.9.99.1752585665 and Tuleap Enterprise Edition prior to 16.8-6 and 16.9-5, users may potentially access confidential information from artifacts that they are not authorized to view. This is fixed in Tuleap Community Edition prior to version 16.9.99.1752585665 and Tuleap Enterprise Edition prior to 16.8-6 and 16.9-5.	4.3	More Details
CVE-2025-8263	A vulnerability was found in prettier up to 3.6.2. It has been declared as problematic. Affected by this vulnerability is the function parseNestedCSS of the file src/language-css/parser-postcss.js. The manipulation of the argument node leads to inefficient regular expression complexity. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-54532	In JetBrains TeamCity before 2025.07 improper access control allowed disclosure of build settings via snapshot dependencies	4.3	More Details
CVE-2025-8226	A vulnerability was found in yanyutao0402 ChanCMS up to 3.1.2. It has been classified as problematic. Affected is an unknown function of the file /sysApp/find. The manipulation of the argument accessKey/secretKey leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.3 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2025-6730	The Bonanza – WooCommerce Free Gifts Lite plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the xlo_optin_call() function in all versions up to, and including, 1.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to set the opt in status to success.	4.3	More Details
CVE-			More

2025-54533	In JetBrains TeamCity before 2025.07 improper access control allowed disclosure of build settings via VCS configuration	4.3	Details
CVE-2025-4976	An issue has been discovered in GitLab EE affecting all versions from 17.0 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that, under certain circumstances, could have allowed an attacker to access internal notes in GitLab Duo responses.	4.3	More Details
CVE-2025-54596	Abnormal Security /v1.0/rbac/users_v2/{USER_ID}/ before 2025-02-19 allows downgrading the privileges of other user accounts.	4.3	More Details
CVE-2025-1299	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 18.0.5, all versions starting from 18.1 before 18.1.3, all versions starting from 18.2 before 18.2.1 that, under circumstances, could have allowed an unauthorized user to read deployment job logs by sending a crafted request.	4.3	More Details
CVE-2025-54139	HAX CMS allows users to manage their microsite universe with a NodeJS or PHP backend. In haxcms-nodejs versions 11.0.12 and below and in haxcms-php versions 11.0.7 and below, all pages within the HAX CMS application do not contain headers to prevent other websites from loading the site within an iframe. This applies to both the CMS and generated sites. An unauthenticated attacker can load the standalone login page or other sensitive functionality within an iframe, performing a UI redressing attack (clickjacking). This can be used to perform social engineering attacks to attempt to coerce users into performing unintended actions within the HAX CMS application. This is fixed in haxcms-nodejs version 11.0.13 and haxcms-php 11.0.8.	4.3	More Details
CVE-2025-0765	An issue has been discovered in GitLab CE/EE affecting all versions from 17.9 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that could have allowed an unauthorized user to access custom service desk email addresses.	4.3	More Details
CVE-2025-7001	An issue has been discovered in GitLab CE/EE affecting all versions from 15.0 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that could have allowed priviledged users to access certain resource_group information through the API which should have been unavailable.	4.3	More Details
CVE-2025-5449	A flaw was found in the SFTP server message decoding logic of libssh. The issue occurs due to an incorrect packet length check that allows an integer overflow when handling large payload sizes on 32-bit systems. This issue leads to failed memory allocation and causes the server process to crash, resulting in a denial of service.	4.3	More Details
CVE-2025-54566	hw/pci/pcie_sriov.c in QEMU through 10.0.3 has a migration state inconsistency, a related issue to CVE-2024-26327.	4.2	More Details
CVE-2025-54567	hw/pci/pcie_sriov.c in QEMU through 10.0.3 mishandles the VF Enable bit write mask, a related issue to CVE-2024-26327.	4.2	More Details
CVE-2025-54558	OpenAI Codex CLI before 0.9.0 auto-approves ripgrep (aka rg) execution even with the --pre or --hostname-bin or --search-zip or -z flag.	4.1	More Details
CVE-2025-32019	Harbor is an open source trusted cloud native registry project that stores, signs, and scans content. Versions 2.11.2 and below, as well as versions 2.12.0-rc1 and 2.13.0-rc1, contain a vulnerability where the markdown field in the info tab page can be exploited to inject XSS code. This is fixed in versions 2.11.3 and 2.12.3.	4.1	More Details
CVE-2023-53158	The gix-transport crate before 0.36.1 for Rust allows command execution via the "gix clone 'ssh://-oProxyCommand=open$IFS" substring. NOTE: this was discovered before CVE-2024-32884, a similar vulnerability (involving a username field) that is more difficult to exploit.	4.1	More Details
CVE-2025-4056	A flaw was found in GLib. A denial of service on Windows platforms may occur if an application attempts to spawn a program using long command lines.	3.7	More Details
CVE-2024-58263	The cosmwasm-std crate before 2.0.2 for Rust allows integer overflows that cause incorrect contract calculations.	3.7	More Details
CVE-2025-8205	A vulnerability, which was classified as problematic, has been found in Comodo Dragon up to 134.0.6998.179. Affected by this issue is some unknown functionality of the component IP DNS Leakage Detector. The manipulation leads to cleartext transmission of sensitive information. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-54529	In JetBrains TeamCity before 2025.07 a CSRF was possible in external OAuth login integration	3.7	More Details
CVE-2025-8283	A vulnerability was found in the netavark package, a network stack for containers used with Podman. Due to dns.podman search domain being removed, netavark may return external servers if a valid A/AAAA record is sent as a response. When creating a container with a given name, this name will be used as the hostname for the container itself, as the podman's search domain is not added anymore the container is using the host's resolv.conf, and the DNS resolver will try to look into the search domains contained on it. If one of the domains contain a name with the same hostname as the running container, the connection will forward to unexpected external servers.	3.7	More Details
CVE-2025-	Akamai Rate Control alpha before 2025 allows attackers to send requests above the stipulated thresholds because the rate is measured separately for each edge node.	3.7	More Details

54568			
CVE-2025-8211	A vulnerability was found in Roothub up to 2.6. It has been declared as problematic. Affected by this vulnerability is the function Edit of the file src/main/java/cn/roothub/web/admin/SystemConfigAdminController.java. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-8191	A vulnerability, which was classified as problematic, was found in macrozheng mall up to 1.0.3. Affected is an unknown function of the file /swagger-ui/index.html of the component Swagger UI. The manipulation of the argument configUrl leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor deleted the GitHub issue for this vulnerability without any explanation. Afterwards the vendor was contacted early about this disclosure via email but did not respond in any way.	3.5	More Details
CVE-2025-8155	A vulnerability has been found in D-Link DCS-6010L 1.15.03 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /vb.htm of the component Management Application. The manipulation of the argument paratest leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2025-8222	A vulnerability, which was classified as problematic, has been found in jerryshensjf JPACookieShop 蛋糕商城JPA版 up to 24a15c02b4f75042c9f7f615a3fed2ec1cefb999. Affected by this issue is some unknown functionality of the file GoodsController.java. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. Multiple endpoints are affected.	3.5	More Details
CVE-2025-8115	A vulnerability has been found in PHPGurukul Taxi Stand Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/new-autoortaxi-entry-form.php. The manipulation of the argument registrationnumber/licensenumber leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-8167	A vulnerability was found in code-projects Church Donation System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/edit_members.php. The manipulation of the argument fname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2025-46686	Redis through 8.0.3 allows memory consumption via a multi-bulk command composed of many bulks, sent by an authenticated user. This occurs because the server allocates memory for the command arguments of every bulk, even when the command is skipped because of insufficient permissions. NOTE: this is disputed by the Supplier because abuse of the commands network protocol is not a violation of the Redis Security Model.	3.5	More Details
CVE-2025-8129	A vulnerability, which was classified as problematic, was found in KoaJS Koa up to 3.0.0. Affected is the function back in the library lib/response.js of the component HTTP Header Handler. The manipulation of the argument Referrer leads to open redirect. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-8224	A vulnerability has been found in GNU Binutils 2.44 and classified as problematic. This vulnerability affects the function bfd_elf_get_str_section of the file bfd/elf.c of the component BFD Library. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The name of the patch is db856d41004301b3a56438efd957ef5cabb91530. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-8225	A vulnerability was found in GNU Binutils 2.44 and classified as problematic. This issue affects the function process_debug_info of the file binutils/dwarf.c of the component DWARF Section Handler. The manipulation leads to memory leak. Attacking locally is a requirement. The identifier of the patch is e51fdff7d2e538c0e5accdd65649ac68e6e0ddd4. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-0249	HCL IEM is affected by an improper invalidation of access or JWT token vulnerability. A token was not invalidated which may allow attackers to access sensitive data without authorization.	3.3	More Details
CVE-2024-58266	The shlex crate before 1.2.1 for Rust allows unquoted and unescaped instances of the { and \xa0 characters, which may facilitate command injection.	3.2	More Details
CVE-2024-58264	The serde-json-wasm crate before 1.0.1 for Rust allows stack consumption via deeply nested JSON data.	3.2	More Details
CVE-2025-8206	A vulnerability, which was classified as problematic, was found in Comodo Dragon up to 134.0.6998.179. This affects an unknown part of the component IP DNS Leakage Detector. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2024-58265	The snow crate before 0.9.5 for Rust, when stateful TransportState is used, allows incrementing a nonce and thereby denying message delivery.	3.1	More Details
CVE-2025-8204	A vulnerability classified as problematic was found in Comodo Dragon up to 134.0.6998.179. Affected by this vulnerability is an unknown functionality of the component HSTS Handler. The manipulation leads to security check for standard. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-8260	A vulnerability has been found in Vaelsys 4.1.0 and classified as problematic. This vulnerability affects unknown code of the file /grid/vgrid_server.php of the component MD4 Hash Handler. The manipulation of the argument xajaxargs leads to use of weak hash. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not	3.1	More Details

	respond in any way.		
CVE-2023-53161	The buffered-reader crate before 1.1.5 for Rust allows out-of-bounds array access and a panic.	2.9	More Details
CVE-2025-43712	JHipster before v.8.9.0 allows privilege escalation via a modified authorities parameter. Upon registering in the JHipster portal and logging in as a standard user, the authorities parameter in the response from the api/account endpoint contains the value ROLE_USER. By manipulating the authorities parameter and changing its value to ROLE_ADMIN, the privilege is successfully escalated to an Admin level. This allowed the access to all admin-related functionalities in the application. NOTE: this is disputed by the Supplier because there is no privilege escalation in the context of the JHipster backend (the report only demonstrates that, after using JHipster to generate an application, one can make a non-functional admin screen visible in the front end of that application).	2.9	More Details
CVE-2024-58261	The sequoia-openpgp crate 1.13.0 before 1.21.0 for Rust allows an infinite loop of "Reading a cert: Invalid operation: Not a Key packet" messages for RawCertParser operations that encounter an unsupported primary key type.	2.9	More Details
CVE-2024-58262	The curve25519-dalek crate before 4.1.3 for Rust has a constant-time operation on elliptic curve scalars that is removed by LLVM.	2.9	More Details
CVE-2023-53160	The sequoia-openpgp crate before 1.16.0 for Rust allows out-of-bounds array access and a panic.	2.9	More Details
CVE-2025-0251	HCL IEM is affected by a concurrent login vulnerability. The application allows multiple concurrent sessions using the same user credentials, which may introduce security risks.	2.6	More Details
CVE-2025-0252	HCL IEM is affected by a password in cleartext vulnerability. Sensitive information is transmitted without adequate protection, potentially exposing it to unauthorized access during transit.	2.6	More Details
CVE-2025-0250	HCL IEM is affected by an authorization token sent in cookie vulnerability. A token used for authentication and authorization is being handled in a manner that may increase its exposure to security risks.	2.2	More Details
CVE-2025-0253	HCL IEM is affected by a cookie attribute not set vulnerability due to inconsistency of certain security-related configurations which could increase exposure to potential vulnerabilities.	2.0	More Details
CVE-2025-38475	In the Linux kernel, the following vulnerability has been resolved: smc: Fix various oops due to inet_sock type confusion. syzbot reported weird splats [0][1] in cipso_v4_sock_setattr() while freeing inet_sk(sk)->inet_opt. The address was freed multiple times even though it was read-only memory. cipso_v4_sock_setattr() did nothing wrong, and the root cause was type confusion. The cited commit made it possible to create smc_sock as an INET socket. The issue is that struct smc_sock does not have struct inet_sock as the first member but hijacks AF_INET and AF_INET6 sk_family, which confuses various places. In this case, inet_sock.inet_opt was actually smc_sock.clcsk_data_ready(), which is an address of a function in the text segment. $ pahole -C inet_sock vmlinux struct inet_sock { ... struct ip_options_rcu * inet_opt; /* 784 8 */ $ pahole -C smc_sock vmlinux struct smc_sock { ... void (*clcsk_data_ready)(struct sock *); /* 784 8 */ The same issue for another field was reported before. [2][3] At that time, an ugly hack was suggested [4], but it makes both INET and SMC code error-prone and hard to change. Also, yet another variant was fixed by a hacky commit 98d4435efcbf3 ("net/smc: prevent NULL pointer dereference in txopt_get"). Instead of papering over the root cause by such hacks, we should not allow non-INET socket to reuse the INET infra. Let's add inet_sock as the first member of smc_sock. [0]: kvfree_call_rcu(): Double-freed call. rcu_head 000000006921da73 WARNING: CPU: 0 PID: 6718 at mm/slab_common.c:1956 kvfree_call_rcu+0x94/0x3f0 mm/slab_common.c:1955 Modules linked in: CPU: 0 UID: 0 PID: 6718 Comm: syz.0.17 Tainted: G W 6.16.0-rc4-syzkaller-g7482bb149b9f #0 PREEMPT Tainted: [W]=WARN Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : kvfree_call_rcu+0x94/0x3f0 mm/slab_common.c:1955 lr : kvfree_call_rcu+0x94/0x3f0 mm/slab_common.c:1955 sp : ffff8000a03a7730 x29: ffff8000a03a7730 x28: 00000000fffffff5 x27: 1fffe000184823d3 x26: dfff800000000000 x25: ffff0000c2411e9e x24: ffff0000dd88da00 x23: ffff8000891ac9a0 x22: 00000000ffffffea x21: ffff8000891ac9a0 x20: ffff8000891ac9a0 x19: ffff80008afc2480 x18: 00000000ffffffff x17: 0000000000000000 x16: ffff80008ae642c8 x15: ffff700011ede14c x14: 1ffff00011ede14c x13: 0000000000000004 x12: ffffffffffffffff x11: ffff700011ede14c x10: 0000000000ff0100 x9 : 5fa3c1ffaf0ff000 x8 : 5fa3c1ffaf0ff000 x7 : 0000000000000001 x6 : 0000000000000001 x5 : ffff8000a03a7078 x4 : ffff80008f766c20 x3 : ffff80008054d360 x2 : 0000000000000000 x1 : 0000000000000201 x0 : 0000000000000000 Call trace: kvfree_call_rcu+0x94/0x3f0 mm/slab_common.c:1955 (P) cipso_v4_sock_setattr+0x2f0/0x3f4 net/ipv4/cipso_ipv4.c:1914 netlbl_sock_setattr+0x240/0x334 net/netlabel/netlabel_kapi.c:1000 smack_netlbl_add+0xa8/0x158 security/smack/smack_lsm.c:2581 smack_inode_setsecurity+0x378/0x430 security/smack/smack_lsm.c:2912 security_inode_setsecurity+0x118/0x3c0 security/security.c:2706 __vfs_setxattr_noperm+0x174/0x5c4 fs/xattr.c:251 __vfs_setxattr_locked+0x1ec/0x218 fs/xattr.c:295 vfs_setxattr+0x158/0x2ac fs/xattr.c:321 do_setxattr fs/xattr.c:636 [inline] file_setxattr+0x1b8/0x294 fs/xattr.c:646 path_setxattrat+0x2ac/0x320 fs/xattr.c:711 __do_sys_fsetxattr fs/xattr.c:761 [inline] __se_sys_fsetxattr fs/xattr.c:758 [inline] __arm64_sys_fsetxattr+0xc0/0xdc fs/xattr.c:758 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x98/0x2b8 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x130/0x23c arch/arm64/kernel/syscall.c:132 do_el0_svc+0x48/0x58 arch/arm64/kernel/syscall.c:151 el0_svc+0x58/0x180 arch/arm64/kernel/entry-common.c:879 el0t_64_sync_handler+0x84/0x12c arch/arm64/kernel/entry-common.c:898 el0t_64_sync+0x198/0x19c arch/arm64/kernel/entry.S:600 [---truncated---	N/A	More Details
CVE-2025-38474	In the Linux kernel, the following vulnerability has been resolved: usb: net: sierra: check for no status endpoint The driver checks for having three endpoints and having bulk in and out endpoints, but not that the third endpoint is interrupt input. Rectify the omission.	N/A	More Details

CVE-2025-38476	In the Linux kernel, the following vulnerability has been resolved: rpl: Fix use-after-free in rpl_do_srh_inline(). Running lwt_dst_cache_ref_loop.sh in selftest with KASAN triggers the splat below [0]. rpl_do_srh_inline() fetches ipv6_hdr(skb) and accesses it after skb_cow_head(), which is illegal as the header could be freed then. Let's fix it by making oldhdr to a local struct instead of a pointer. [0]: [root@fedora net]# ./lwt_dst_cache_ref_loop.sh ... TEST: rpl (input) [57.631529] == BUG: KASAN: slab-use-after-free in rpl_do_srh_inline.isra.0 (net/ipv6/rpl_iptunnel.c:174) Read of size 40 at addr ffff888122bf96d8 by task ping6/1543 CPU: 50 UID: 0 PID: 1543 Comm: ping6 Not tainted 6.16.0-rc5-01302-gfadd1e6231b1 #23 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <IRQ> dump_stack_lvl (lib/dump_stack.c:122) print_report (mm/kasan/report.c:409 mm/kasan/report.c:521) kasan_report (mm/kasan/report.c:221 mm/kasan/report.c:636) kasan_check_range (mm/kasan/generic.c:175 (discriminator 1) mm/kasan/generic.c:189 (discriminator 1)) __asan_memmove (mm/kasan/shadow.c:94 (discriminator 2)) rpl_do_srh_inline.isra.0 (net/ipv6/rpl_iptunnel.c:174) rpl_input (net/ipv6/rpl_iptunnel.c:201 net/ipv6/rpl_iptunnel.c:282) lwtunnel_input (net/core/lwtunnel.c:459) ipv6_rcv (./include/net/dst.h:471 (discriminator 1) ./include/net/dst.h:469 (discriminator 1) net/ipv6/ip6_input.c:79 (discriminator 1) ./include/linux/netfilter.h:317 (discriminator 1) ./include/linux/netfilter.h:311 (discriminator 1) net/ipv6/ip6_input.c:311 (discriminator 1)) __netif_receive_skb_one_core (net/core/dev.c:5967) process_backlog (./include/linux/rcupdate.h:869 net/core/dev.c:6440) __napi_poll.constprop.0 (net/core/dev.c:7452) net_rx_action (net/core/dev.c:7518 net/core/dev.c:7643) handle_softirqs (kernel/softirq.c:579) do_softirq (kernel/softirq.c:480 (discriminator 20)) </IRQ> <TASK> __local_bh_enable_ip (kernel/softirq.c:407) __dev_queue_xmit (net/core/dev.c:4740) ip6_finish_output2 (./include/linux/netdevice.h:3358 ./include/net/neighbour.h:526 ./include/net/neighbour.h:540 net/ipv6/ip6_output.c:141) ip6_finish_output (net/ipv6/ip6_output.c:215 net/ipv6/ip6_output.c:226) ip6_output (./include/linux/netfilter.h:306 net/ipv6/ip6_output.c:248) ip6_send_skb (net/ipv6/ip6_output.c:1983) rawv6_sendmsg (net/ipv6/raw.c:588 net/ipv6/raw.c:918) __sys_sendto (net/socket.c:714 (discriminator 1) net/socket.c:729 (discriminator 1) net/socket.c:2228 (discriminator 1)) __x64_sys_sendto (net/socket.c:2231) do_syscall_64 (arch/x86/entry/syscall_64.c:63 (discriminator 1) arch/x86/entry/syscall_64.c:94 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f68cffb2a06 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 RSP: 002b:00007ffefb7c53d0 EFLAGS: 00000202 ORIG_RAX: 000000000000002c RAX: ffffffffffffffda RBX: 0000564cd69f10a0 RCX: 00007f68cffb2a06 RDX: 0000000000000040 RSI: 0000564cd69f10a4 RDI: 0000000000000003 RBP: 00007ffefb7c53f0 R08: 0000564cd6a032ac R09: 000000000000001c R10: 0000000000000000 R11: 0000000000000202 R12: 0000564cd69f10a4 R13: 0000000000000040 R14: 00007ffefb7c66e0 R15: 0000564cd69f10a0 </TASK> Allocated by task 1543: kasan_save_stack (mm/kasan/common.c:48) kasan_save_track (mm/kasan/common.c:60 (discriminator 1) mm/kasan/common.c:69 (discriminator 1)) __kasan_slab_alloc (mm/kasan/common.c:319 mm/kasan/common.c:345) kmem_cache_alloc_node_noprof (./include/linux/kasan.h:250 mm/slub.c:4148 mm/slub.c:4197 mm/slub.c:4249) kmalloc_reserve (net/core/skbuff.c:581 (discriminator 88)) __alloc_skb (net/core/skbuff.c:669) __ip6_append_data (net/ipv6/ip6_output.c:1672 (discriminator 1)) ip6_ ---truncated---	N/A	More Details
CVE-2025-38473	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix null-ptr-deref in l2cap_sock_resume_cb() syzbot reported null-ptr-deref in l2cap_sock_resume_cb(). [0] l2cap_sock_resume_cb() has a similar problem that was fixed by commit 1bff51ea59a9 ("Bluetooth: fix use-after-free error in lock_sock_nested()"). Since both l2cap_sock_kill() and l2cap_sock_resume_cb() are executed under l2cap_sock_resume_cb(), we can avoid the issue simply by checking if chan->data is NULL. Let's not access to the killed socket in l2cap_sock_resume_cb(). [0]: BUG: KASAN: null-ptr-deref in instrument_atomic_write include/linux/instrumented.h:82 [inline] BUG: KASAN: null-ptr-deref in clear_bit include/asm-generic/bitops/instrumented-atomic.h:41 [inline] BUG: KASAN: null-ptr-deref in l2cap_sock_resume_cb+0xb4/0x17c net/bluetooth/l2cap_sock.c:1711 Write of size 8 at addr 0000000000000570 by task kworker/u9:0/52 CPU: 1 UID: 0 PID: 52 Comm: kworker/u9:0 Not tainted 6.16.0-rc4-syzkaller-g7482bb149b9f #0 PREEMPT Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Workqueue: hci0 hci_rx_work Call trace: show_stack+0x2c/0x3c arch/arm64/kernel/stacktrace.c:501 (C) __dump_stack+0x30/0x40 lib/dump_stack.c:94 dump_stack_lvl+0xd8/0x12c lib/dump_stack.c:120 print_report+0x58/0x84 mm/kasan/report.c:524 kasan_report+0xb0/0x110 mm/kasan/report.c:634 check_region_inline mm/kasan/generic.c:-1 [inline] kasan_check_range+0x264/0x2a4 mm/kasan/generic.c:189 __kasan_check_write+0x20/0x30 mm/kasan/shadow.c:37 instrument_atomic_write include/linux/instrumented.h:82 [inline] clear_bit include/asm-generic/bitops/instrumented-atomic.h:41 [inline] l2cap_sock_resume_cb+0xb4/0x17c net/bluetooth/l2cap_sock.c:1711 l2cap_security_cfm+0x524/0xea0 net/bluetooth/l2cap_core.c:7357 hci_auth_cfm include/net/bluetooth/hci_core.h:2092 [inline] hci_auth_complete_evt+0x2e8/0xa4c net/bluetooth/hci_event.c:3514 hci_event_func net/bluetooth/hci_event.c:7511 [inline] hci_event_packet+0x650/0xe9c net/bluetooth/hci_event.c:7565 hci_rx_work+0x320/0xb18 net/bluetooth/hci_core.c:4070 process_one_work+0x7e8/0x155c kernel/workqueue.c:3238 process_scheduled_works kernel/workqueue.c:3321 [inline] worker_thread+0x958/0xed8 kernel/workqueue.c:3402 kthread+0x5fc/0x75c kernel/kthread.c:464 ret_from_fork+0x10/0x20 arch/arm64/kernel/entry.S:847	N/A	More Details
CVE-2025-54371	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-54426	Polkadot Frontier is an Ethereum and EVM compatibility layer for Polkadot and Substrate. In versions prior to commit 36f70d1, the Curve25519Add and Curve25519ScalarMul precompiles incorrectly handle invalid Ristretto point representations. Instead of returning an error, they silently treat invalid input bytes as the Ristretto identity element, leading to potentially incorrect cryptographic results. This is fixed in commit 36f70d1.	N/A	More Details
CVE-2025-38477	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_qfq: Fix race condition on qfq_aggregate A race condition can occur when 'agg' is modified in qfq_change_agg (called during qfq_enqueue) while other threads access it concurrently. For example, qfq_dump_class may trigger a NULL dereference, and qfq_delete_class may cause a use-after-free. This patch addresses the issue by: 1. Moved qfq_destroy_class into the critical section. 2. Added sch_tree_lock protection to qfq_dump_class and qfq_dump_class_stats.	N/A	More Details
CVE-2025-54662	Rejected reason: Not used	N/A	More Details
CVE-2025-54420	Rejected reason: This CVE is a duplicate of CVE-2025-8129.	N/A	More Details

CVE-2024-42645	An issue in FlashMQ v1.14.0 allows attackers to cause an assertion failure via sending a crafted retain message, leading to a Denial of Service (DoS).	N/A	More Details
CVE-2024-42644	FlashMQ v1.14.0 was discovered to contain an assertion failure in the function PublishCopyFactory::getNewPublish, which occurs when the QoS value of the publish object is greater than 0.	N/A	More Details
CVE-2025-7458	An integer overflow in the sqlite3KeyInfoFromExprList function in SQLite versions 3.39.2 through 3.41.1 allows an attacker with the ability to execute arbitrary SQL statements to cause a denial of service or disclose sensitive information from process memory via a crafted SELECT statement with a large number of expressions in the ORDER BY clause.	N/A	More Details
CVE-2025-54422	Sandboxie is a sandbox-based isolation software for 32-bit and 64-bit Windows NT-based operating systems. In versions 1.16.1 and below, a critical security vulnerability exists in password handling mechanisms. During encrypted sandbox creation, user passwords are transmitted via shared memory, exposing them to potential interception. The vulnerability is particularly severe during password modification operations, where both old and new passwords are passed as plaintext command-line arguments to the Imbox process without any encryption or obfuscation. This implementation flaw allows any process within the user session, including unprivileged processes, to retrieve these sensitive credentials by reading the command-line arguments, thereby bypassing standard privilege requirements and creating a significant security risk. This is fixed in version 1.16.2.	N/A	More Details
CVE-2025-40686	Reflected Cross-Site Scripting (XSS) in Human Resource Management System version 1.0. This vulnerability could allow an attacker to execute JavaScript code in the victim's browser by sending a malicious URL through the 'employeeid' parameter in/detailview.php.	N/A	More Details
CVE-2025-40685	Reflected Cross-Site Scripting (XSS) in Human Resource Management System version 1.0. This vulnerability could allow an attacker to execute JavaScript code in the victim's browser by sending a malicious URL through the 'searcstate' parameter in/state.php.	N/A	More Details
CVE-2025-40684	Reflected Cross-Site Scripting (XSS) in Human Resource Management System version 1.0. This vulnerability could allow an attacker to execute JavaScript code in the victim's browser by sending a malicious URL through the 'searccountry' parameter in/country.php.	N/A	More Details
CVE-2025-40683	Reflected Cross-Site Scripting (XSS) in Human Resource Management System version 1.0. This vulnerability could allow an attacker to execute JavaScript code in the victim's browser by sending a malicious URL through the 'searccity' parameter in /city.php.	N/A	More Details
CVE-2025-40682	SQL injection vulnerability in Human Resource Management System version 1.0, which allows an attacker to retrieve, create, update and delete databases via the “city” and “state” parameters in the /controller/ccity.php endpoint.	N/A	More Details
CVE-2025-43881	Improper validation of specified quantity in input issue exists in Real-time Bus Tracking System versions prior to 1.1. If exploited, a denial of service (DoS) condition may be caused by an attacker who can log in to the administrative page of the affected product.	N/A	More Details
CVE-2025-53649	"SwitchBot" App for iOS/Android contains an insertion of sensitive information into log file vulnerability in versions V6.24 through V9.12. If this vulnerability is exploited, sensitive user information may be exposed to an attacker who has access to the application logs.	N/A	More Details
CVE-2025-54666	Rejected reason: Not used	N/A	More Details
CVE-2025-54665	Rejected reason: Not used	N/A	More Details
CVE-2025-54664	Rejected reason: Not used	N/A	More Details
CVE-2025-54432	Rejected reason: This CVE is a duplicate of another CVE. See CVE-2018-25031 and CVE-2021-46708.	N/A	More Details
CVE-2025-5922	Access to TSplus Remote Access Admin Tool is restricted to administrators (unless "Disable UAC" option is enabled) and requires a PIN code. In versions below v18.40.6.17 the PIN's hash is stored in a system registry accessible to regular users, making it possible to perform a brute-force attack using rainbow tables, since the hash is not salted. LTS (Long-Term Support) versions also received patches in v17.2025.6.27 and v16.2025.6.27 releases.	N/A	More Details
CVE-2025-2179	An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect™ App on Linux devices enables a locally authenticated non administrative user to disable the app even if the GlobalProtect app configuration would not normally permit them to do so. The GlobalProtect app on Windows, macOS, iOS, Android, Chrome OS and GlobalProtect UWP app are not affected.	N/A	More Details
CVE-2025-43487	A potential privilege escalation through Sudo vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The firmware flaw does not properly implement access controls. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43485	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The vulnerability could potentially allow a privileged user to retrieve credentials from the log files. HP has addressed the issue in the latest software update.	N/A	More Details

CVE-2025-43486	A potential stored cross-site scripting vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The website allows user input to be stored and rendered without proper sanitization. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-54126	The WebAssembly Micro Runtime's (WAMR) iwasm package is the executable binary built with WAMR VMcore which supports WebAssembly System Interface (WASI) and command line interface. In versions 2.4.0 and below, iwasm uses --addr-pool with an IPv4 address that lacks a subnet mask, allowing the system to accept all IP addresses. This can unintentionally expose the service to all incoming connections and bypass intended access restrictions. Services relying on --addr-pool for restricting access by IP may unintentionally become open to all external connections. This may lead to unauthorized access in production deployments, especially when users assume that specifying an IP without a subnet mask implies a default secure configuration. This is fixed in version 2.4.1.	N/A	More Details
CVE-2025-4674	The go command may execute unexpected commands when operating in untrusted VCS repositories. This occurs when possibly dangerous VCS configuration is present in repositories. This can happen when a repository was fetched via one VCS (e.g. Git), but contains metadata for another VCS (e.g. Mercurial). Modules which are retrieved using the go command line, i.e. via "go get", are not affected.	N/A	More Details
CVE-2025-40600	Use of Externally-Controlled Format String vulnerability in the SonicOS SSL VPN interface allows a remote unauthenticated attacker to cause service disruption.	N/A	More Details
CVE-2025-53102	Discourse is an open-source community discussion platform. Prior to version 3.4.7 on the `stable` branch and version 3.5.0.beta.8 on the `tests-passed` branch, upon issuing a physical security key for 2FA, the server generates a WebAuthn challenge, which the client signs. The challenge is not cleared from the user’s session after authentication, potentially allowing reuse and increasing security risk. This is fixed in versions 3.4.7 and 3.5.0.beta.8.	N/A	More Details
CVE-2025-43488	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The vulnerability could allow a bypass of the application's XSS filter by submitting untrusted characters. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-53711	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WlanNetworkRpm.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2025-43489	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The vulnerability could deserialize untrusted data without validation. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-54120	PCL (Plain Craft Launcher) Community Edition is a Minecraft launcher. In PCL CE versions 2.12.0-beta.5 to 2.12.0-beta.9, the login credentials used during the third-party login process are accidentally recorded in the local log file. Although the log file is not automatically uploaded or shared, if the user manually sends the log file, there is a risk of leakage. This is fixed in version 2.12.0-beta.10.	N/A	More Details
CVE-2025-53715	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/Wan6to4TunnelCfgRpm.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2025-53714	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WzdWlanSiteSurveyRpm_AP.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2025-53713	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WlanNetworkRpm_APC.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2025-53712	A vulnerability has been found in TP-Link TL-WR841N V11. The vulnerability exists in the /userRpm/WlanNetworkRpm_AP.htm file due to missing input parameter validation, which may lead to the buffer overflow to cause a crash of the web service and result in a denial-of-service (DoS) condition. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2025-54663	Rejected reason: Not used	N/A	More Details
CVE-2025-54661	Rejected reason: Not used	N/A	More Details
CVE-2025-38478	In the Linux kernel, the following vulnerability has been resolved: comedi: Fix initialization of data for instructions that write to subdevice Some Comedi subdevice instruction handlers are known to access instruction data elements beyond the first `insn->n` elements in some cases. The `do_insn_ioctl()` and `do_insnlist_ioctl()` functions allocate at least `MIN_SAMPLES` (16) data elements to deal with this, but they do not initialize all of that. For Comedi instruction codes that write to the subdevice, the first `insn->n` data elements are copied from user-space, but the remaining elements are left uninitialized. That could be a problem if the subdevice instruction handler reads the uninitialized data. Ensure that the first `MIN_SAMPLES` elements are initialized before calling these instruction handlers, filling the uncopied elements with 0. For `do_insnlist_ioctl()`, the same data buffer elements are used for handling a list of instructions, so ensure the first `MIN_SAMPLES` elements are initialized for each instruction that writes to the subdevice.	N/A	More Details

CVE-2025-54429	Polkadot Frontier is an Ethereum and EVM compatibility layer for Polkadot and Substrate. There are various account address types in Frontier, e.g. precompiled contracts, smart contracts, and externally owned accounts. Some EVM mechanisms should be unreachable by certain types of accounts for safety. For precompiles to be callable by smart contracts they must be explicitly configured as CallableByContract. If this configuration is absent, then the precompile should be unreachable via smart contract accounts. In commits prior to 0822030, the underlying implementation of CallableByContract which returned the AddressType was incorrect. It considered the contract address running under CREATE or CREATE2 to be AddressType::EOA rather than correctly as AddressType::Contract. The issue only affects users who use custom precompile implementations that utilize AddressType::EOA and AddressType::Contract. It's not directly exploitable in any of the predefined precompiles in Frontier. This is fixed in version 0822030.	N/A	More Details
CVE-2025-38494	In the Linux kernel, the following vulnerability has been resolved: HID: core: do not bypass hid_hw_raw_request hid_hw_raw_request() is actually useful to ensure the provided buffer and length are valid. Directly calling in the low level transport driver function bypassed those checks and allowed invalid paramto be used.	N/A	More Details
CVE-2025-38493	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Fix crash in timerlat_dump_stack() We have observed kernel panics when using timerlat with stack saving, with the following dmesg output: memcpy: detected buffer overflow: 88 byte write of buffer size 0 WARNING: CPU: 2 PID: 8153 at lib/string_helpers.c:1032 __fortify_report+0x55/0xa0 CPU: 2 UID: 0 PID: 8153 Comm: timerlatu/2 Kdump: loaded Not tainted 6.15.3-200.fc42.x86_64 #1 PREEMPT(lazy) Call Trace: <TASK> ? trace_buffer_lock_reserve+0x2a/0x60 __fortify_panic+0xd/0xf __timerlat_dump_stack.cold+0xd/0xd timerlat_dump_stack.part.0+0x47/0x80 timerlat_fd_read+0x36d/0x390 vfs_read+0xe2/0x390 ? syscall_exit_to_user_mode+0x1d5/0x210 ksys_read+0x73/0xe0 do_syscall_64+0x7b/0x160 ? exc_page_fault+0x7e/0x1a0 entry_SYSCALL_64_after_hwframe+0x76/0x7e __timerlat_dump_stack() constructs the ftrace stack entry like this: struct stack_entry *entry; ... memcpy(&entry->caller, fstack->calls, size); entry->size = fstack->nr_entries; Since commit e7186af7fb26 ("tracing: Add back FORTIFY_SOURCE logic to kernel_stack event structure"), struct stack_entry marks its caller field with __counted_by(size). At the time of the memcpy, entry->size contains garbage from the ringbuffer, which under some circumstances is zero, triggering a kernel panic by buffer overflow. Populate the size field before the memcpy so that the out-of-bounds check knows the correct size. This is analogous to __ftrace_trace_stack().	N/A	More Details
CVE-2025-38492	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix race between cache write completion and ALL_QUEUED being set When netfslib is issuing subrequests, the subrequests start processing immediately and may complete before we reach the end of the issuing function. At the end of the issuing function we set NETFS_RREQ_ALL_QUEUED to indicate to the collector that we aren't going to issue any more subreqs and that it can do the final notifications and cleanup. Now, this isn't a problem if the request is synchronous (NETFS_RREQ_OFFLOAD_COLLECTION is unset) as the result collection will be done in-thread and we're guaranteed an opportunity to run the collector. However, if the request is asynchronous, collection is primarily triggered by the termination of subrequests queuing it on a workqueue. Now, a race can occur here if the app thread sets ALL_QUEUED after the last subrequest terminates. This can happen most easily with the copy2cache code (as used by Ceph) where, in the collection routine of a read request, an asynchronous write request is spawned to copy data to the cache. Folios are added to the write request as they're unlocked, but there may be a delay before ALL_QUEUED is set as the write subrequests may complete before we get there. If all the write subreqs have finished by the ALL_QUEUED point, no further events happen and the collection never happens, leaving the request hanging. Fix this by queuing the collector after setting ALL_QUEUED. This is a bit heavy-handed and it may be sufficient to do it only if there are no extant subreqs. Also add a tracepoint to cross-reference both requests in a copy-to-request operation and add a trace to the netfs_rreq tracepoint to indicate the setting of ALL_QUEUED.	N/A	More Details
CVE-2025-38491	In the Linux kernel, the following vulnerability has been resolved: mptcp: make fallback action and fallback decision atomic Syzkaller reported the following splat: WARNING: CPU: 1 PID: 7704 at net/mptcp/protocol.h:1223 __mptcp_do_fallback net/mptcp/protocol.h:1223 [inline] WARNING: CPU: 1 PID: 7704 at net/mptcp/protocol.h:1223 mptcp_do_fallback net/mptcp/protocol.h:1244 [inline] WARNING: CPU: 1 PID: 7704 at net/mptcp/protocol.h:1223 check_fully_established net/mptcp/options.c:982 [inline] WARNING: CPU: 1 PID: 7704 at net/mptcp/protocol.h:1223 mptcp_incoming_options+0x21a8/0x2510 net/mptcp/options.c:1153 Modules linked in: CPU: 1 UID: 0 PID: 7704 Comm: syz.3.1419 Not tainted 6.16.0-rc3-gbd5ce2324dba #20 PREEMPT(voluntary) Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:__mptcp_do_fallback net/mptcp/protocol.h:1223 [inline] RIP: 0010:mptcp_do_fallback net/mptcp/protocol.h:1244 [inline] RIP: 0010:check_fully_established net/mptcp/options.c:982 [inline] RIP: 0010:mptcp_incoming_options+0x21a8/0x2510 net/mptcp/options.c:1153 Code: 24 18 e8 bb 2a 00 fd e9 1b df ff ff e8 b1 21 0f 00 e8 ec 5f c4 fc 44 0f b7 ac 24 b0 00 00 00 e9 54 f1 ff ff e8 d9 5f c4 fc 90 <0f> 0b 90 e9 b8 f4 ff ff e8 8b 2a 00 fd e9 8d e6 ff ff e8 81 2a 00 RSP: 0018:ffff8880a3f08448 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff8880180a8000 RCX: ffffffff84afcf45 RDX: ffff888090223700 RSI: ffffffff84afdaa7 RDI: 0000000000000001 RBP: ffff888017955780 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000 R13: ffff8880180a8910 R14: ffff8880a3e9d058 R15: 0000000000000000 FS: 00005555791b8500(0000) GS:ffff88811c495000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000110c2800b7 CR3: 0000000058e44000 CR4: 0000000000350ef0 Call Trace: <IRQ> tcp_reset+0x26f/0x2b0 net/ipv4/tcp_input.c:4432 tcp_validate_incoming+0x1057/0x1b60 net/ipv4/tcp_input.c:5975 tcp_rcv_established+0x5b5/0x21f0 net/ipv4/tcp_input.c:6166 tcp_v4_do_rcv+0x5dc/0xa70 net/ipv4/tcp_ipv4.c:1925 tcp_v4_rcv+0x3473/0x44a0 net/ipv4/tcp_ipv4.c:2363 ip_protocol_deliver_rcu+0xba/0x480 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x2f1/0x500 net/ipv4/ip_input.c:233 NF_HOOK include/linux/netfilter.h:317 [inline] NF_HOOK include/linux/netfilter.h:311 [inline] ip_local_deliver+0x1be/0x560 net/ipv4/ip_input.c:254 dst_input include/net/dst.h:469 [inline] ip_rcv_finish net/ipv4/ip_input.c:447 [inline] NF_HOOK include/linux/netfilter.h:317 [inline] NF_HOOK include/linux/netfilter.h:311 [inline] ip_rcv+0x514/0x810 net/ipv4/ip_input.c:567 __netif_receive_skb_one_core+0x197/0x1e0 net/core/dev.c:5975 __netif_receive_skb+0x1f/0x120 net/core/dev.c:6088 process_backlog+0x301/0x1360 net/core/dev.c:6440 __napi_poll.constprop.0+0xba/0x550 net/core/dev.c:7453 napi_poll net/core/dev.c:7517 [inline] net_rx_action+0xb44/0x1010 net/core/dev.c:7644 handle_softirqs+0x1d0/0x770 kernel/softirq.c:579 do_softirq+0x3f/0x90 kernel/softirq.c:480 </IRQ> <TASK> __local_bh_enable_ip+0xed/0x110 kernel/softirq.c:407 local_bh_enable include/linux/bottom_half.h:33 [inline] inet_csk_listen_stop+0x2c5/0x1070 net/ipv4/inet_connection_sock.c:1524 mptcp_check_listen_stop.part.0+0x1cc/0x220 net/mptcp/protocol.c:2985 mptcp_check_listen_stop net/mptcp/mib.h:118 [inline] __mptcp_close+0x9b9/0xbd0 net/mptcp/protocol.c:3000 mptcp_close+0x2f/0x140 net/mptcp/protocol.c:3066 inet_release+0xed/0x200 net/ipv4/af_inet.c:435 inet6_release+0x4f/0x70 net/ipv6/af_inet6.c:487 __sock_release+0xb3/0x270 net/socket.c:649 sock_close+0x1c/0x30 net/socket.c:1439 __fput+0x402/0xb70 fs/file_table.c:465 task_work_run+0x150/0x240 kernel/task_work.c:227 resume_user_mode_work include/linux/resume_user_mode.h:50 [inline] exit_to_user_mode_loop+0xd4 ---truncated---	N/A	More Details

CVE-2025-38490	In the Linux kernel, the following vulnerability has been resolved: net: libwx: remove duplicate page_pool_put_full_page() page_pool_put_full_page() should only be invoked when freeing Rx buffers or building a skb if the size is too short. At other times, the pages need to be reused. So remove the redundant page put. In the original code, double free pages cause kernel panic: [876.949834] __irq_exit_rcu+0xc7/0x130 [876.949836] common_interrupt+0xb8/0xd0 [876.949838] </IRQ> [876.949838] <TASK> [876.949840] asm_common_interrupt+0x22/0x40 [876.949841] RIP: 0010:cpuidle_enter_state+0xc2/0x420 [876.949843] Code: 00 00 e8 d1 1d 5e ff e8 ac f0 ff ff 49 89 c5 0f 1f 44 00 00 31 ff e8 cd fc 5c ff 45 84 ff 0f 85 40 02 00 00 fb 0f 1f 44 00 00 <45> 85 f6 0f 88 84 01 00 00 49 63 d6 48 8d 04 52 48 8d 04 82 49 8d [876.949844] RSP: 0018:ffffaa7340267e78 EFLAGS: 00000246 [876.949845] RAX: ffff9e3f135be000 RBX: 0000000000000002 RCX: 0000000000000000 [876.949846] RDX: 000000cc2dc4cb7c RSI: ffffffff89ee49ae RDI: ffffffff89ef9f9e [876.949847] RBP: ffff9e378f940800 R08: 0000000000000002 R09: 00000000000000ed [876.949848] R10: 000000000000afc8 R11: ffff9e3e9e5a9b6c R12: ffffffff8a6d8580 [876.949849] R13: 000000cc2dc4cb7c R14: 0000000000000002 R15: 0000000000000000 [876.949852] ? cpuidle_enter_state+0xb3/0x420 [876.949855] cpuidle_enter+0x29/0x40 [876.949857] cpuidle_idle_call+0xfd/0x170 [876.949859] do_idle+0x7a/0xc0 [876.949861] cpu_startup_entry+0x25/0x30 [876.949862] start_secondary+0x117/0x140 [876.949864] common_startup_64+0x13e/0x148 [876.949867] </TASK> [876.949868] ---[end trace 0000000000000000]--- [876.949869] ------------[cut here]------------ [876.949870] list_del corruption, ffffead40445a348->next is NULL [876.949873] WARNING: CPU: 14 PID: 0 at lib/list_debug.c:52 __list_del_entry_valid_or_report+0x67/0x120 [876.949875] Modules linked in: snd_hrtimer(E) bnep(E) binfmt_misc(E) amdgpu(E) squashfs(E) vfat(E) loop(E) fat(E) amd_atl(E) snd_hda_codec_realtek(E) intel_rapl_msr(E) snd_hda_codec_generic(E) intel_rapl_common(E) snd_hda_scodec_component(E) snd_hda_codec_hdmi(E) snd_hda_intel(E) edac_mce_amd(E) snd_intel_dspcfg(E) snd_hda_codec(E) snd_hda_core(E) amdxcp(E) kvm_amd(E) snd_hwdep(E) gpu_sched(E) drm_panel_backlight_quirks(E) cec(E) snd_pcm(E) drm_buddy(E) snd_seq_dummy(E) drm_ttm_helper(E) btusb(E) kvm(E) snd_seq_oss(E) btrtl(E) ttm(E) btintel(E) snd_seq_midi(E) btbcm(E) drm_exec(E) snd_seq_midi_event(E) i2c_algo_bit(E) snd_rawmidi(E) bluetooth(E) drm_suballoc_helper(E) irqbypass(E) snd_seq(E) ghash_clmulni_intel(E) sha512_ssse3(E) drm_display_helper(E) aesni_intel(E) snd_seq_device(E) rfkill(E) snd_timer(E) gf128mul(E) drm_client_lib(E) drm_kms_helper(E) snd(E) i2c_piix4(E) joydev(E) soundcore(E) wmi_bmof(E) ccp(E) k10temp(E) i2c_smbus(E) gpio_amdpt(E) i2c_designware_platform(E) gpio_generic(E) sg(E) [876.949914] i2c_designware_core(E) sch_fq_codel(E) parport_pc(E) drm(E) ppdev(E) lp(E) parport(E) fuse(E) nfnetlink(E) ip_tables(E) ext4 crc16 mbcache jbd2 sd_mod sfp mdio_i2c i2c_core txgbe ahci ngbe pcs_xpcs libahci libwx r8169 phylink libata realtek ptp pps_core video wmi [876.949933] CPU: 14 UID: 0 PID: 0 Comm: swapper/14 Kdump: loaded Tainted: G W E 6.16.0-rc2+ #20 PREEMPT(voluntary) [876.949935] Tainted: [W]=WARN, [E]=UNSIGNED_MODULE [876.949936] Hardware name: Micro-Star International Co., Ltd. MS-7E16/X670E GAMING PLUS WIFI (MS-7E16), BIOS 1.90 12/31/2024 [876.949936] RIP: 0010:__list_del_entry_valid_or_report+0x67/0x120 [876.949938] Code: 00 00 00 48 39 7d 08 0f 85 a6 00 00 00 5b b8 01 00 00 00 5d 41 5c e9 73 0d 93 ff 48 89 fe 48 c7 c7 a0 31 e8 89 e8 59 7c b3 ff <0f> 0b 31 c0 5b 5d 41 5c e9 57 0d 93 ff 48 89 fe 48 c7 c7 c8 31 e8 [876.949940] RSP: 0018:ffffaa73405d0c60 EFLAGS: 00010282 [876.949941] RAX: 0000000000000000 RBX: ffffead40445a348 RCX: 0000000000000000 [876.949942] RDX: 0000000000000105 RSI: 00000 ---truncated---	N/A	More Details
CVE-2025-38489	In the Linux kernel, the following vulnerability has been resolved: s390/bpf: Fix bpf_arch_text_poke() with new_addr == NULL again Commit 7ded842b356d ("s390/bpf: Fix bpf_plt pointer arithmetic") has accidentally removed the critical piece of commit c730fce7c70c ("s390/bpf: Fix bpf_arch_text_poke() with new_addr == NULL"), causing intermittent kernel panics in e.g. perf's on_switch() prog to reappear. Restore the fix and add a comment.	N/A	More Details
CVE-2025-38488	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free in crypt_message when using async crypto The CVE-2024-50047 fix removed asynchronous crypto handling from crypt_message(), assuming all crypto operations are synchronous. However, when hardware crypto accelerators are used, this can cause use-after-free crashes: crypt_message() // Allocate the creq buffer containing the req creq = smb2_get_aead_req(..., &req); // Async encryption returns -EINPROGRESS immediately rc = enc ? crypto_aead_encrypt(req) : crypto_aead_decrypt(req); // Free creq while async operation is still in progress kvfree_sensitive(creq, ...); Hardware crypto modules often implement async AEAD operations for performance. When crypto_aead_encrypt/decrypt() returns -EINPROGRESS, the operation completes asynchronously. Without crypto_wait_req(), the function immediately frees the request buffer, leading to crashes when the driver later accesses the freed memory. This results in a use-after-free condition when the hardware crypto driver later accesses the freed request structure, leading to kernel crashes with NULL pointer dereferences. The issue occurs because crypto_alloc_aead() with mask=0 doesn't guarantee synchronous operation. Even without CRYPTO_ALG_ASYNC in the mask, async implementations can be selected. Fix by restoring the async crypto handling: - DECLARE_CRYPTO_WAIT(wait) for completion tracking - aead_request_set_callback() for async completion notification - crypto_wait_req() to wait for operation completion This ensures the request buffer isn't freed until the crypto operation completes, whether synchronous or asynchronous, while preserving the CVE-2024-50047 fix.	N/A	More Details
CVE-2025-38487	In the Linux kernel, the following vulnerability has been resolved: soc: aspeed: lpc-snoop: Don't disable channels that aren't enabled Mitigate e.g. the following: # echo 1e789080.lpc-snoop > /sys/bus/platform/drivers/aspeed-lpc-snoop/unbind ... [120.363594] Unable to handle kernel NULL pointer dereference at virtual address 00000004 when write [120.373866] [00000004] *pgd=00000000 [120.377910] Internal error: Oops: 805 [#1] SMP ARM [120.383306] CPU: 1 UID: 0 PID: 315 Comm: sh Not tainted 6.15.0-rc1-00009-g926217bc7d7d-dirty #20 NONE ... [120.679543] Call trace: [120.679559] misc_deregister from aspeed_lpc_snoop_remove+0x84/0xac [120.692462] aspeed_lpc_snoop_remove from platform_remove+0x28/0x38 [120.700996] platform_remove from device_release_driver_internal+0x188/0x200 ...	N/A	More Details
CVE-2025-38486	In the Linux kernel, the following vulnerability has been resolved: soundwire: Revert "soundwire: qcom: Add set_channel_map api support" This reverts commit 7796c97df6b1b2206681a07f3c80f6023a6593d5. This patch broke Dragonboard 845c (sdm845). I see: Unexpected kernel BRK exception at EL1 Internal error: BRK handler: 00000000f20003e8 [#1] SMP pc : qcom_swrm_set_channel_map+0x7c/0x80 [soundwire_qcom] lr : snd_soc_dai_set_channel_map+0x34/0x78 Call trace: qcom_swrm_set_channel_map+0x7c/0x80 [soundwire_qcom] (P) sdm845_dai_init+0x18c/0x2e0 [snd_soc_sdm845] snd_soc_link_init+0x28/0x6c snd_soc_bind_card+0x5f4/0xb0c snd_soc_register_card+0x148/0x1a4 devm_snd_soc_register_card+0x50/0xb0 sdm845_snd_platform_probe+0x124/0x148 [snd_soc_sdm845] platform_probe+0x6c/0xd0 really_probe+0xc0/0x2a4 __driver_probe_device+0x7c/0x130 driver_probe_device+0x40/0x118 __device_attach_driver+0xc4/0x108 bus_for_each_drv+0x8c/0xf0 __device_attach+0xa4/0x198 device_initial_probe+0x18/0x28 bus_probe_device+0xb8/0xbc deferred_probe_work_func+0xac/0xfc process_one_work+0x244/0x658 worker_thread+0x1b4/0x360 kthread+0x148/0x228 ret_from_fork+0x10/0x20 Kernel panic - not syncing: BRK handler: Fatal exception Dan has also reported following issues with the original patch https://lore.kernel.org/all/33fe8fe7-719a-405a-9ed2-d9f816ce1d57@sabinyo.mountain/ Bug #1: The zeroeth element of ctrl->pconfig[] is supposed to be unused. We start counting at 1. However this code sets ctrl->pconfig[0].ch_mask = 128. Bug #2: There are SLIM_MAX_TX_PORTS (16) elements in tx_ch[]	N/A	More Details

	array but only QCOM_SDW_MAX_PORTS + 1 (15) in the ctrl->pconfig[] array so it corrupts memory like Yongqin Liu pointed out. Bug 3: Like Jie Gan pointed out, it erases all the tx information with the rx information.		
CVE-2025-38485	In the Linux kernel, the following vulnerability has been resolved: iio: accel: fxls8962af: Fix use after free in fxls8962af_fifo_flush fxls8962af_fifo_flush() uses indio_dev->active_scan_mask (with iio_for_each_active_channel()) without making sure the indio_dev stays in buffer mode. There is a race if indio_dev exits buffer mode in the middle of the interrupt that flushes the fifo. Fix this by calling synchronize_irq() to ensure that no interrupt is currently running when disabling buffer mode. Unable to handle kernel NULL pointer dereference at virtual address 00000000 when read [...] _find_first_bit_le from fxls8962af_fifo_flush+0x17c/0x290 fxls8962af_fifo_flush from fxls8962af_interrupt+0x80/0x178 fxls8962af_interrupt from irq_thread_fn+0x1c/0x7c irq_thread_fn from irq_thread+0x110/0x1f4 irq_thread from kthread+0xe0/0xfc kthread from ret_from_fork+0x14/0x2c	N/A	More Details
CVE-2025-38484	In the Linux kernel, the following vulnerability has been resolved: iio: backend: fix out-of-bound write The buffer is set to 80 character. If a caller write more characters, count is truncated to the max available space in "simple_write_to_buffer". But afterwards a string terminator is written to the buffer at offset count without boundary check. The zero termination is written OUT-OF-BOUND. Add a check that the given buffer is smaller then the buffer to prevent.	N/A	More Details
CVE-2025-38483	In the Linux kernel, the following vulnerability has been resolved: comedi: das16m1: Fix bit shift out of bounds When checking for a supported IRQ number, the following test is used: /* only irqs 2, 3, 4, 5, 6, 7, 10, 11, 12, 14, and 15 are valid */ if ((1 << it->options[1]) & 0xdcfc) { However, `it->options[i]` is an unchecked `int` value from userspace, so the shift amount could be negative or out of bounds. Fix the test by requiring `it->options[1]` to be within bounds before proceeding with the original test.	N/A	More Details
CVE-2025-38482	In the Linux kernel, the following vulnerability has been resolved: comedi: das6402: Fix bit shift out of bounds When checking for a supported IRQ number, the following test is used: /* IRQs 2,3,5,6,7, 10,11,15 are valid for "enhanced" mode */ if ((1 << it->options[1]) & 0x8cec) { However, `it->options[i]` is an unchecked `int` value from userspace, so the shift amount could be negative or out of bounds. Fix the test by requiring `it->options[1]` to be within bounds before proceeding with the original test. Valid `it->options[1]` values that select the IRQ will be in the range [1,15]. The value 0 explicitly disables the use of interrupts.	N/A	More Details
CVE-2025-38481	In the Linux kernel, the following vulnerability has been resolved: comedi: Fail COMEDI_INSNLIST ioctl if n_insns is too large The handling of the `COMEDI_INSNLIST` ioctl allocates a kernel buffer to hold the array of `struct comedi_insn`, getting the length from the `n_insns` member of the `struct comedi_insnlist` supplied by the user. The allocation will fail with a WARNING and a stack dump if it is too large. Avoid that by failing with an `-EINVAL` error if the supplied `n_insns` value is unreasonable. Define the limit on the `n_insns` value in the `MAX_INSNS` macro. Set this to the same value as `MAX_SAMPLES` (65536), which is the maximum allowed sum of the values of the member `n` in the array of `struct comedi_insn`, and sensible comedi instructions will have an `n` of at least 1.	N/A	More Details
CVE-2025-38480	In the Linux kernel, the following vulnerability has been resolved: comedi: Fix use of uninitialized data in insn_rw_emulate_bits() For Comedi `INSN_READ` and `INSN_WRITE` instructions on "digital" subdevices (subdevice types `COMEDI_SUBD_DI`, `COMEDI_SUBD_DO`, and `COMEDI_SUBD_DIO`), it is common for the subdevice driver not to have `insn_read` and `insn_write` handler functions, but to have an `insn_bits` handler function for handling Comedi `INSN_BITS` instructions. In that case, the subdevice's `insn_read` and/or `insn_write` function handler pointers are set to point to the `insn_rw_emulate_bits()` function by `__comedi_device_postconfig()`. For `INSN_WRITE`, `insn_rw_emulate_bits()` currently assumes that the supplied `data[0]` value is a valid copy from user memory. It will at least exist because `do_insnlist_ioctl()` and `do_insn_ioctl()` in "comedi_fops.c" ensure at lease `MIN_SAMPLES` (16) elements are allocated. However, if `insn->n` is 0 (which is allowable for `INSN_READ` and `INSN_WRITE` instructions, then `data[0]` may contain uninitialized data, and certainly contains invalid data, possibly from a different instruction in the array of instructions handled by `do_insnlist_ioctl()`. This will result in an incorrect value being written to the digital output channel (or to the digital input/output channel if configured as an output), and may be reflected in the internal saved state of the channel. Fix it by returning 0 early if `insn->n` is 0, before reaching the code that accesses `data[0]`. Previously, the function always returned 1 on success, but it is supposed to be the number of data samples actually read or written up to `insn->n`, which is 0 in this case.	N/A	More Details
CVE-2025-38495	In the Linux kernel, the following vulnerability has been resolved: HID: core: ensure the allocated report buffer can contain the reserved report ID When the report ID is not used, the low level transport drivers expect the first byte to be 0. However, currently the allocated buffer not account for that extra byte, meaning that instead of having 8 guaranteed bytes for implement to be working, we only have 7.	N/A	More Details
CVE-2025-38496	In the Linux kernel, the following vulnerability has been resolved: dm-bufio: fix sched in atomic context If "try_verify_in_tasklet" is set for dm-verity, DM_BUFIO_CLIENT_NO_SLEEP is enabled for dm-bufio. However, when bufio tries to evict buffers, there is a chance to trigger scheduling in spin_lock_bh, the following warning is hit: BUG: sleeping function called from invalid context at drivers/md/dm-bufio.c:2745 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 123, name: kworker/2:2 preempt_count: 201, expected: 0 RCU nest depth: 0, expected: 0 4 locks held by kworker/2:2/123: #0: ffff88800a2d1548 ((wq_completion)dm_bufio_cache){....}-{0:0}, at: process_one_work+0xe46/0x1970 #1: ffffc90000d97d20 ((work_completion)(&dm_bufio_replacement_work)){....}-{0:0}, at: process_one_work+0x763/0x1970 #2: ffffffff8555b528 (dm_bufio_clients_lock){....}-{3:3}, at: do_global_cleanup+0x1ce/0x710 #3: ffff88801d5820b8 (&c->spinlock){....}-{2:2}, at: do_global_cleanup+0x2a5/0x710 Preemption disabled at: [<0000000000000000>] 0x0 CPU: 2 UID: 0 PID: 123 Comm: kworker/2:2 Not tainted 6.16.0-rc3-g90548c634bd0 #305 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 Workqueue: dm_bufio_cache do_global_cleanup Call Trace: <TASK> dump_stack_lvl+0x53/0x70 __might_resched+0x360/0x4e0 do_global_cleanup+0x2f5/0x710 process_one_work+0x7db/0x1970 worker_thread+0x518/0xea0 kthread+0x359/0x690 ret_from_fork+0xf3/0x1b0 ret_from_fork_asm+0x1a/0x30 </TASK> That can be reproduced by: veritysetup format --data-block-size=4096 --hash-block-size=4096 /dev/vda /dev/vdb SIZE=$(blockdev --getsz /dev/vda) dmsetup create myverity -r --table "0 $SIZE verity 1 /dev/vda /dev/vdb 4096 4096 <data_blocks> 1 sha256 <root_hash> <salt> 1 try_verify_in_tasklet" mount /dev/dm-0 /mnt -o ro echo 102400 > /sys/module/dm_bufio/parameters/max_cache_size_bytes [read files in /mnt]	N/A	More Details
CVE-2025-38497	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: configfs: Fix OOB read on empty string write When writing an empty string to either 'qw_sign' or 'landingPage' sysfs attributes, the store functions attempt to access page[l - 1] before validating that the length 'l' is greater than zero. This patch fixes the vulnerability by adding a check at the beginning of os_desc_qw_sign_store() and webusb_landingPage_store() to handle the zero-length input case gracefully by returning	N/A	More Details

	immediately.		
CVE-2025-6250	Prior to 25.4.270.0, when wmic.exe is elevated with a full admin token the user can stop the Defendpoint service, bypassing anti-tamper protections. Once the service is disabled, the malicious user can add themselves to Administrators group and run any process with elevated permissions.	N/A	More Details
CVE-2025-54427	Polkadot Frontier is an Ethereum and EVM compatibility layer for Polkadot and Substrate. The extrinsic note_min_gas_price_target is an inherent extrinsic, meaning only the block producer can call it. To ensure correctness, the ProvideInherent trait should be implemented for each inherent, which includes the check_inherent call. This allows other nodes to verify if the input (in this case, the target value) is correct. However, prior to commit a754b3d, the check_inherent function has not been implemented for note_min_gas_price_target. This lets the block producer set the target value without verification. The target is then used to set the MinGasPrice, which has an upper and lower bound defined in the on_initialize hook. The block producer can set the target to the upper bound. Which also increases the upper and lower bounds for the next block. Over time, this could result in continuously raising the gas price, making contract execution too expensive and ineffective for users. An attacker could use this flaw to manipulate the gas price, potentially leading to significantly inflated transaction fees. Such manipulation could render contract execution prohibitively expensive for users, effectively resulting in a denial-of-service condition for the network. This is fixed in version a754b3d.	N/A	More Details
CVE-2025-38471	In the Linux kernel, the following vulnerability has been resolved: tls: always refresh the queue when reading sock After recent changes in net-next TCP compacts skbs much more aggressively. This unearthed a bug in TLS where we may try to operate on an old skb when checking if all skbs in the queue have matching decrypt state and geometry. BUG: KASAN: slab-use-after-free in tls_strp_check_rcv+0x898/0x9a0 [tls] (net/tls/tls_strp.c:436 net/tls/tls_strp.c:530 net/tls/tls_strp.c:544) Read of size 4 at addr ffff888013085750 by task tls/13529 CPU: 2 UID: 0 PID: 13529 Comm: tls Not tainted 6.16.0-rc5-virtme Call Trace: kasan_report+0xca/0x100 tls_strp_check_rcv+0x898/0x9a0 [tls] tls_rx_rec_wait+0x2c9/0x8d0 [tls] tls_sw_recvmsg+0x40f/0x1aa0 [tls] inet_recvmsg+0x1c3/0x1f0 Always reload the queue, fast path is to have the record in the queue when we wake, anyway (IOW the path going down "if !strp->stm.full_len").	N/A	More Details
CVE-2025-54299	A stored XSS vulnerability in No Boss Testimonials component 1.0.0-3.0.0 and 4.0.0-4.0.2 for Joomla was discovered.	N/A	More Details
CVE-2025-54298	A stored XSS vulnerability in CommentBox component 1.0.0-1.1.0 for Joomla was discovered.	N/A	More Details
CVE-2025-43023	A potential security vulnerability has been identified in the HP Linux Imaging and Printing Software documentation. This potential vulnerability is due to the use of a weak code signing key, Digital Signature Algorithm (DSA).	N/A	More Details
CVE-2025-7676	DLL hijacking of all PE32 executables when run on Windows for ARM64 CPU architecture. This allows an attacker to execute code, if the attacker can plant a DLL in the same directory as the executable. Vulnerable versions of Windows 11 for ARM attempt to load Base DLLs that would ordinarily not be loaded from the application directory. Fixed in release 24H2, but present in all earlier versions of Windows 11 for ARM CPUs.	N/A	More Details
CVE-2025-2297	Prior to version 25.4.270.0, a local authenticated attacker can manipulate user profile files to add illegitimate challenge response codes into the local user registry under certain conditions. This allows users with the ability to edit their user profile files to elevate their privileges to administrator.	N/A	More Details
CVE-2025-8070	The Windows service configuration of ABP and AES contains an unquoted ImagePath registry value vulnerability. This allows a local attacker to execute arbitrary code by placing a malicious executable in a predictable location such as C:\Program.exe. If the service runs with elevated privileges, exploitation results in privilege escalation to SYSTEM level. This vulnerability arises from an unquoted service path affecting systems where the executable resides in a path containing spaces. Affected products and versions include: ABP 2.0.7.6130 and earlier as well as AES 1.0.6.6133 and earlier.	N/A	More Details
CVE-2025-53696	iSTAR Ultra performs a firmware verification on boot, however the verification does not inspect certain portions of the firmware. These firmware parts may contain malicious code. Tested up to firmware 6.9.2, later firmwares are also possibly affected.	N/A	More Details
CVE-2025-30125	An issue was discovered on Marbella KR8s Dashcam FF 2.0.8 devices. All dashcams were shipped with the same default credentials of 12345678, which creates an insecure-by-default condition. For users who change their passwords, it's limited to 8 characters. These short passwords can be cracked in 8 hours via low-end commercial cloud resources.	N/A	More Details
CVE-2025-53695	OS Command Injection in iSTAR Ultra products web application allows an authenticated attacker to gain even more privileged access ('root' user) to the device firmware.	N/A	More Details
CVE-2025-30133	An issue was discovered on IROAD Dashcam FX2 devices. Bypass of Device Pairing/Registration can occur. It requires device registration via the "IROAD X View" app for authentication, but its HTTP server lacks this restriction. Once connected to the dashcam's Wi-Fi network via the default password ("qwertyuiop"), an attacker can directly access the HTTP server at http://192.168.10.1 without undergoing the pairing process. Additionally, no alert is triggered on the device when an attacker connects, making this intrusion completely silent.	N/A	More Details
CVE-2025-30126	An issue was discovered on Marbella KR8s Dashcam FF 2.0.8 devices. Via port 7777 without any need to pair or press a physical button, a remote attacker can disable recording, delete recordings, or even disable battery protection to cause a flat battery to essentially disable the car from being used. During the process of changing these settings, there are no indications or sounds on the dashcam to alert the dashcam owner that someone else is making those changes.	N/A	More Details
CVE-2025-30124	An issue was discovered on Marbella KR8s Dashcam FF 2.0.8 devices. When a new SD card is inserted into the dashcam, the existing password is written onto the SD card in cleartext automatically. An attacker with temporary access to the dashcam can switch the SD card to steal this password.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack: fix crash due to removal of		

CVE-2025-38472	uninitialised entry A crash in conntrack was reported while trying to unlink the conntrack entry from the hash bucket list: [exception RIP: __nf_ct_delete_from_lists+172] [..] #7 [ff539b5a2b043aa0] nf_ct_delete at ffffffffc124d421 [nf_conntrack] #8 [ff539b5a2b043ad0] nf_ct_gc_expired at ffffffffc124d999 [nf_conntrack] #9 [ff539b5a2b043ae0] __nf_conntrack_find_get at ffffffffc124efbc [nf_conntrack] [..] The nf_conn struct is marked as allocated from slab but appears to be in a partially initialised state: ct hlist pointer is garbage; looks like the ct hash value (hence crash). ct->status is equal to IPS_CONFIRMED|IPS_DYING, which is expected ct->timeout is 30000 (=30s), which is unexpected. Everything else looks like normal udp conntrack entry. If we ignore ct->status and pretend its 0, the entry matches those that are newly allocated but not yet inserted into the hash: - ct hlist pointers are overloaded and store/cache the raw tuple hash - ct->timeout matches the relative time expected for a new udp flow rather than the absolute 'jiffies' value. If it were not for the presence of IPS_CONFIRMED, __nf_conntrack_find_get() would have skipped the entry. Theory is that we did hit following race: cpu x cpu y cpu z found entry E found entry E E is expired <preemption> nf_ct_delete() return E to rcu slab init_conntrack E is re-inited, ct->status set to 0 reply tuplehash hnnode.pprev stores hash value. cpu y found E right before it was deleted on cpu x. E is now re-inited on cpu z. cpu y was preempted before checking for expiry and/or confirm bit. ->refcnt set to 1 E now owned by skb ->timeout set to 30000 If cpu y were to resume now, it would observe E as expired but would skip E due to missing CONFIRMED bit. nf_conntrack_confirm gets called sets: ct->status |= CONFIRMED This is wrong: E is not yet added to hashtable. cpu y resumes, it observes E as expired but CONFIRMED: <resumes> nf_ct_expired() -> yes (ct->timeout is 30s) confirmed bit set. cpu y will try to delete E from the hashtable: nf_ct_delete() -> set DYING bit __nf_ct_delete_from_lists Even this scenario doesn't guarantee a crash: cpu z still holds the table bucket lock(s) so y blocks: wait for spinlock held by z CONFIRMED is set but there is no guarantee ct will be added to hash: "chaintoolong" or "clash resolution" logic both skip the insert step. reply hnnode.pprev still stores the hash value. unlocks spinlock return NF_DROP <unblocks, then crashes on hlist_nulls_del_rcu pprev> In case CPU z does insert the entry into the hashtable, cpu y will unlink E again right away but no crash occurs. Without 'cpu y' race, 'garbage' hlist is of no consequence: ct refcnt remains at 1, eventually skb will be free'd and E gets destroyed via: nf_conntrack_put -> nf_conntrack_destroy -> nf_ct_destroy. To resolve this, move the IPS_CONFIRMED assignment after the table insertion but before the unlock. Pablo points out that the confirm-bit-store could be reordered to happen before hlist add resp. the timeout fixup, so switch to set_bit and before_atomic memory barrier to prevent this. It doesn't matter if other CPUs can observe a newly inserted entry right before the CONFIRMED bit was set: Such event cannot be distinguished from above "E is the old incarnation" case: the entry will be skipped. Also change nf_ct_should_gc() to first check the confirmed bit. The gc sequence is: 1. Check if entry has expired, if not skip to next entry 2. Obtain a reference to the expired entry. 3. Call nf_ct_should_gc() to double-check step 1. nf_ct_should_gc() is thus called only for entries that already failed an expiry check. After this patch, once the confirmed bit check pas ---truncated---	N/A	More Details
CVE-2025-54366	FreeScout is a lightweight free open source help desk and shared inbox built with PHP (Laravel framework). In versions 1.8.185 and below, there is a critical deserialization vulnerability in the /conversation/ajax endpoint that allows authenticated users with knowledge of the APP_KEY to achieve remote code execution. The vulnerability occurs when the application processes the attachments_all and attachments POST parameters through the insecure Helper::decrypt() function, which performs unsafe deserialization of user-controlled data without proper validation. This flaw enables attackers to create arbitrary objects and manipulate their properties, leading to complete compromise of the web application. This is fixed in version 1.8.186.	N/A	More Details
CVE-2025-38470	In the Linux kernel, the following vulnerability has been resolved: net: vlan: fix VLAN 0 refcount imbalance of toggling filtering during runtime Assuming the "rx-vlan-filter" feature is enabled on a net device, the 8021q module will automatically add or remove VLAN 0 when the net device is put administratively up or down, respectively. There are a couple of problems with the above scheme. The first problem is a memory leak that can happen if the "rx-vlan-filter" feature is disabled while the device is running: # ip link add bond1 up type bond mode 0 # ethtool -K bond1 rx-vlan-filter off # ip link del dev bond1 When the device is put administratively down the "rx-vlan-filter" feature is disabled, so the 8021q module will not remove VLAN 0 and the memory will be leaked [1]. Another problem that can happen is that the kernel can automatically delete VLAN 0 when the device is put administratively down despite not adding it when the device was put administratively up since during that time the "rx-vlan-filter" feature was disabled. null-ptr-unref or bug_on[2] will be triggered by unregister_vlan_dev() for refcount imbalance if toggling filtering during runtime: $ ip link add bond0 type bond mode 0 $ ip link add link bond0 name vlan0 type vlan id 0 protocol 802.1q $ ethtool -K bond0 rx-vlan-filter off $ ifconfig bond0 up $ ethtool -K bond0 rx-vlan-filter on $ ifconfig bond0 down $ ip link del vlan0 Root cause is as below: step1: add vlan0 for real_dev, such as bond, team. register_vlan_dev vlan_vid_add(real_dev,htons(ETH_P_8021Q),0) //refcnt=1 step2: disable vlan filter feature and enable real_dev step3: change filter from 0 to 1 vlan_device_event vlan_filter_push_vids ndo_vlan_rx_add_vid //No refcnt added to real_dev vlan0 step4: real_dev down vlan_device_event vlan_vid_del(dev, htons(ETH_P_8021Q), 0); //refcnt=0 vlan_info_rcu_free //free vlan0 step5: delete vlan0 unregister_vlan_dev BUG_ON(!vlan_info); //vlan_info is null Fix both problems by noting in the VLAN info whether VLAN 0 was automatically added upon NETDEV_UP and based on that decide whether it should be deleted upon NETDEV_DOWN, regardless of the state of the "rx-vlan-filter" feature. [1] unreferenced object 0xffff8880068e3100 (size 256): comm "ip", pid 384, jiffies 4296130254 hex dump (first 32 bytes): 00 20 30 0d 80 88 ff ff 00 00 00 00 00 00 00 00 . 0............ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... backtrace (crc 81ce31fa): __kmalloc_cache_noprof+0x2b5/0x340 vlan_vid_add+0x434/0x940 vlan_device_event.cold+0x75/0xa8 notifier_call_chain+0xca/0x150 __dev_notify_flags+0xe3/0x250 rtnl_configure_link+0x193/0x260 rtnl_newlink_create+0x383/0x8e0 __rtnl_newlink+0x22c/0xa40 rtnl_newlink+0x627/0xb00 rtnetlink_rcv_msg+0x6fb/0xb70 netlink_rcv_skb+0x11f/0x350 netlink_unicast+0x426/0x710 netlink_sendmsg+0x75a/0xc20 __sock_sendmsg+0xc1/0x150 ____sys_sendmsg+0x5aa/0x7b0 ___sys_sendmsg+0xfc/0x180 [2] kernel BUG at net/8021q/vlan.c:99! Oops: invalid opcode: 0000 [#1] SMP KASAN PTI CPU: 0 UID: 0 PID: 382 Comm: ip Not tainted 6.16.0-rc3 #61 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 RIP: 0010:unregister_vlan_dev (net/8021q/vlan.c:99 (discriminator 1)) RSP: 0018:ffff88810badf310 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff88810da84000 RCX: ffffffffb47ceb9a RDX: dffffc0000000000 RSI: 0000000000000008 RDI: ffff88810e8b43c8 RBP: 0000000000000000 R08: 0000000000000000 R09: fffffbfff6cefe80 R10: ffffffffb677f407 R11: ffff88810badf3c0 R12: ffff88810e8b4000 R13: 0000000000000000 R14: ffff88810642a5c0 R15: 000000000000017e FS: 00007f1ff68c20c0(0000) GS:ffff888163a24000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f1ff5dad240 CR3: 0000000107e56000 CR4: 00000000000006f0 Call Trace: <TASK ---truncated---	N/A	More Details
CVE-2025-38384	In the Linux kernel, the following vulnerability has been resolved: mtd: spinand: fix memory leak of ECC engine conf Memory allocated for the ECC engine conf is not released during spinand cleanup. Below kmemleak trace is seen for this memory leak: unreferenced object 0xffffff80064f00e0 (size 8): comm "swapper/0", pid 1, jiffies 4294937458 hex dump (first 8 bytes): 00 00 00 00 00 00 00 00 .... backtrace (crc 0): kmemleak_alloc+0x30/0x40 __kmalloc_cache_noprof+0x208/0x3c0 spinand_ondie_ecc_init_ctx+0x114/0x200 nand_ecc_init_ctx+0x70/0xa8 nanddev_ecc_engine_init+0xec/0x27c spinand_probe+0xa2c/0x1620 spi_mem_probe+0x130/0x21c spi_probe+0xf0/0x170 really_probe+0x17c/0x6e8 __driver_probe_device+0x17c/0x21c driver_probe_device+0x58/0x180 __device_attach_driver+0x15c/0x1f8	N/A	More Details

	bus_for_each_drv+0xec/0x150 __device_attach+0x188/0x24c device_initial_probe+0x10/0x20 bus_probe_device+0x11c/0x160 Fix the leak by calling nanddev_ecc_engine_cleanup() inside spinand_cleanup().		
CVE-2025-38404	In the Linux kernel, the following vulnerability has been resolved: usb: typec: displayport: Fix potential deadlock The deadlock can occur due to a recursive lock acquisition of `cros_typec_altmode_data::mutex`. The call chain is as follows: 1. cros_typec_altmode_work() acquires the mutex 2. typec_altmode_vdm() -> dp_altmode_vdm() -> 3. typec_altmode_exit() -> cros_typec_altmode_exit() 4. cros_typec_altmode_exit() attempts to acquire the mutex again To prevent this, defer the `typec_altmode_exit()` call by scheduling it rather than calling it directly from within the mutex-protected context.	N/A	More Details
CVE-2025-38403	In the Linux kernel, the following vulnerability has been resolved: vsock/vmci: Clear the vmci transport packet properly when initializing it In vmci_transport_packet_init memset the vmci_transport_packet before populating the fields to avoid any uninitialised data being left in the structure.	N/A	More Details
CVE-2025-38402	In the Linux kernel, the following vulnerability has been resolved: idpf: return 0 size for RSS key if not supported Returning -EOPNOTSUPP from function returning u32 is leading to cast and invalid size value as a result. -EOPNOTSUPP as a size probably will lead to allocation fail. Command: ethtool -x eth0 It is visible on all devices that don't have RSS caps set. [136.615917] Call Trace: [136.615921] <TASK> [136.615927] ? __warn+0x89/0x130 [136.615942] ? __alloc_frozen_pages_noprof+0x322/0x330 [136.615953] ? report_bug+0x164/0x190 [136.615968] ? handle_bug+0x58/0x90 [136.615979] ? exc_invalid_op+0x17/0x70 [136.615987] ? asm_exc_invalid_op+0x1a/0x20 [136.616001] ? rss_prepare_get.constprop.0+0xb9/0x170 [136.616016] ? __alloc_frozen_pages_noprof+0x322/0x330 [136.616028] __alloc_pages_noprof+0xe/0x20 [136.616038] ___kmalloc_large_node+0x80/0x110 [136.616072] __kmalloc_large_node_noprof+0x1d/0xa0 [136.616081] __kmalloc_noprof+0x32c/0x4c0 [136.616098] ? rss_prepare_get.constprop.0+0xb9/0x170 [136.616105] rss_prepare_get.constprop.0+0xb9/0x170 [136.616114] ethnl_default_doit+0x107/0x3d0 [136.616131] genl_family_rcv_msg_doit+0x100/0x160 [136.616147] genl_rcv_msg+0x1b8/0x2c0 [136.616156] ? __pfx_ethnl_default_doit+0x10/0x10 [136.616168] ? __pfx_genl_rcv_msg+0x10/0x10 [136.616176] netlink_rcv_skb+0x58/0x110 [136.616186] genl_rcv+0x28/0x40 [136.616195] netlink_unicast+0x19b/0x290 [136.616206] netlink_sendmsg+0x222/0x490 [136.616215] __sys_sendto+0x1fd/0x210 [136.616233] __x64_sys_sendto+0x24/0x30 [136.616242] do_syscall_64+0x82/0x160 [136.616252] ? __sys_recvmsg+0x83/0xe0 [136.616265] ? syscall_exit_to_user_mode+0x10/0x210 [136.616275] ? do_syscall_64+0x8e/0x160 [136.616282] ? __count_memcg_events+0xa1/0x130 [136.616295] ? count_memcg_events.constprop.0+0x1a/0x30 [136.616306] ? handle_mm_fault+0xae/0x2d0 [136.616319] ? do_user_addr_fault+0x379/0x670 [136.616328] ? clear_bhb_loop+0x45/0xa0 [136.616340] ? clear_bhb_loop+0x45/0xa0 [136.616349] ? clear_bhb_loop+0x45/0xa0 [136.616359] entry_SYSCALL_64_after_hwframe+0x76/0x7e [136.616369] RIP: 0033:0x7fd30ba7b047 [136.616376] Code: 0c 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b8 0f 1f 00 f3 0f 1e fa 80 3d bd d5 0c 00 00 41 89 ca 74 10 b8 2c 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 71 c3 55 48 83 ec 30 44 89 4c 24 2c 4c 89 44 [136.616381] RSP: 002b:00007ffde1796d68 EFLAGS: 00000202 ORIG_RAX: 000000000000002c [136.616388] RAX: ffffffffffffffda RBX: 000055d7bd89f2a0 RCX: 00007fd30ba7b047 [136.616392] RDX: 0000000000000028 RSI: 000055d7bd89f3b0 RDI: 0000000000000003 [136.616396] RBP: 00007ffde1796e10 R08: 00007fd30bb4e200 R09: 000000000000000c [136.616399] R10: 0000000000000000 R11: 0000000000000202 R12: 000055d7bd89f340 [136.616403] R13: 000055d7bd89f3b0 R14: 000055d78943f200 R15: 0000000000000000	N/A	More Details
CVE-2025-38401	In the Linux kernel, the following vulnerability has been resolved: mtk-sd: Prevent memory corruption from DMA map failure If msdc_prepare_data() fails to map the DMA region, the request is not prepared for data receiving, but msdc_start_data() proceeds the DMA with previous setting. Since this will lead a memory corruption, we have to stop the request operation soon after the msdc_prepare_data() fails to prepare it.	N/A	More Details
CVE-2025-38400	In the Linux kernel, the following vulnerability has been resolved: nfs: Clean up /proc/net/rpc/nfs when nfs_fs_proc_net_init() fails. syzbot reported a warning below [1] following a fault injection in nfs_fs_proc_net_init(). [0] When nfs_fs_proc_net_init() fails, /proc/net/rpc/nfs is not removed. Later, rpc_proc_exit() tries to remove /proc/net/rpc, and the warning is logged as the directory is not empty. Let's handle the error of nfs_fs_proc_net_init() properly. [0]: FAULT_INJECTION: forcing a failure. name failslab, interval 1, probability 0, space 0, times 0 CPU: 1 UID: 0 PID: 6120 Comm: syz.2.27 Not tainted 6.16.0-rc1-syzkaller-00010-g2c4a1f3fe03e #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123) should_fail_ex (lib/fault-inject.c:73 lib/fault-inject.c:174) should_failslab (mm/failslab.c:46) kmem_cache_alloc_noprof (mm/slub.c:4178 mm/slub.c:4204) __proc_create (fs/proc/generic.c:427) proc_create_reg (fs/proc/generic.c:554) proc_create_net_data (fs/proc/proc_net.c:120) nfs_fs_proc_net_init (fs/nfs/client.c:1409) nfs_net_init (fs/nfs/inode.c:2600) ops_init (net/core/net_namespace.c:138) setup_net (net/core/net_namespace.c:443) copy_net_ns (net/core/net_namespace.c:576) create_new_namespaces (kernel/nsproxy.c:110) unshare_nsproxy_namespaces (kernel/nsproxy.c:218 (discriminator 4)) ksys_unshare (kernel/fork.c:3123) __x64_sys_unshare (kernel/fork.c:3190) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) </TASK> [1]: remove_proc_entry: removing non-empty directory 'net/rpc', leaking at least 'nfs' WARNING: CPU: 1 PID: 6120 at fs/proc/generic.c:727 remove_proc_entry+0x45e/0x530 fs/proc/generic.c:727 Modules linked in: CPU: 1 UID: 0 PID: 6120 Comm: syz.2.27 Not tainted 6.16.0-rc1-syzkaller-00010-g2c4a1f3fe03e #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 RIP: 0010:remove_proc_entry+0x45e/0x530 fs/proc/generic.c:727 Code: 3c 02 00 0f 85 85 00 00 00 48 8b 93 d8 00 00 00 4d 89 f0 4c 89 e9 48 c7 c6 40 ba a2 8b 48 c7 c7 60 b9 a2 8b e8 33 81 1d ff 90 <0f> 0b 90 90 e9 5f fe ff ff e8 04 69 5e ff 90 48 b8 00 00 00 00 00 RSP: 0018:ffffc90003637b08 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffff88805f534140 RCX: ffffffff817a92c8 RDX: ffff88807da99e00 RSI: ffffffff817a92d5 RDI: 0000000000000001 RBP: ffff888033431ac0 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000001 R11: 0000000000000001 R12: ffff888033431a00 R13: ffff888033431ae4 R14: ffff888033184724 R15: dffffc0000000000 FS: 0000555580328500(0000) GS:ffff888124a62000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f71733743e0 CR3: 000000007f618000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> sunrpc_exit_net+0x46/0x90 net/sunrpc/sunrpc_syms.c:76 ops_exit_list net/core/net_namespace.c:200 [inline] ops_undo_list+0x2eb/0xab0 net/core/net_namespace.c:253 setup_net+0x2e1/0x510 net/core/net_namespace.c:457 copy_net_ns+0x2a6/0x5f0 net/core/net_namespace.c:574 create_new_namespaces+0x3ea/0xa90 kernel/nsproxy.c:110 unshare_nsproxy_namespaces+0xc0/0x1f0 kernel/nsproxy.c:218 ksys_unshare+0x45b/0xa40 kernel/fork.c:3121 __do_sys_unshare kernel/fork.c:3192 [inline] __se_sys_unshare kernel/fork.c:3190 [inline] __x64_sys_unshare+0x31/0x40 kernel/fork.c:3190 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x490 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fa1a6b8e929 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c ---truncated---	N/A	More Details

CVE-2025-38399	In the Linux kernel, the following vulnerability has been resolved: scsi: target: Fix NULL pointer dereference in core_scsi3_decode_spec_i_port() The function core_scsi3_decode_spec_i_port(), in its error code path, unconditionally calls core_scsi3_lunacl_undepend_item() passing the dest_se_deve pointer, which may be NULL. This can lead to a NULL pointer dereference if dest_se_deve remains unset. SPC-3 PR SPEC_I_PT: Unable to locate dest_tpg Unable to handle kernel paging request at virtual address dfff800000000012 Call trace: core_scsi3_lunacl_undepend_item+0x2c/0xf0 [target_core_mod] (P) core_scsi3_decode_spec_i_port+0x120c/0x1c30 [target_core_mod] core_scsi3_emulate_pro_register+0x6b8/0xcd8 [target_core_mod] target_scsi3_emulate_pr_out+0x56c/0x840 [target_core_mod] Fix this by adding a NULL check before calling core_scsi3_lunacl_undepend_item()	N/A	More Details
CVE-2025-38398	In the Linux kernel, the following vulnerability has been resolved: spi: spi-qpic-snand: reallocate BAM transactions Using the mtd_nandbiterrs module for testing the driver occasionally results in weird things like below. 1. swiotlb mapping fails with the following message: [85.926216] qcom_snand 79b0000.spi: swiotlb buffer is full (sz: 4294967294 bytes), total 512 (slots), used 0 (slots) [85.932937] qcom_snand 79b0000.spi: failure in mapping desc [87.999314] qcom_snand 79b0000.spi: failure to write raw page [87.999352] mtd_nandbiterrs: error: write_oob failed (-110) Rebooting the board after this causes a panic due to a NULL pointer dereference. 2. If the swiotlb mapping does not fail, rebooting the board may result in a different panic due to a bad spinlock magic: [256.104459] BUG: spinlock bad magic on CPU#3, procd/2241 [256.104488] Unable to handle kernel paging request at virtual address ffffffff0000049b ... Investigating the issue revealed that these symptoms are results of memory corruption which is caused by out of bounds access within the driver. The driver uses a dynamically allocated structure for BAM transactions, which structure must have enough space for all possible variations of different flash operations initiated by the driver. The required space heavily depends on the actual number of 'codewords' which is calculated from the pagesize of the actual NAND chip. Although the qcom_nandc_alloc() function allocates memory for the BAM transactions during probe, but since the actual number of 'codewords' is not yet know the allocation is done for one 'codeword' only. Because of this, whenever the driver does a flash operation, and the number of the required transactions exceeds the size of the allocated arrays the driver accesses memory out of the allocated range. To avoid this, change the code to free the initially allocated BAM transactions memory, and allocate a new one once the actual number of 'codewords' required for a given NAND chip is known.	N/A	More Details
CVE-2025-38397	In the Linux kernel, the following vulnerability has been resolved: nvme-multipath: fix suspicious RCU usage warning When I run the NVME over TCP test in virtme-ng, I get the following "suspicious RCU usage" warning in nvme_mpath_add_sysfs_link(): ''' [5.024557][T44] nvmet: Created nvm controller 1 for subsystem nqn.2025-06.org.nvmexpress.mptcp for NQN nqn.2014-08.org.nvmexpress:uuid:f7f6b5e0-ff97-4894-98ac-c85309e0bc77. [5.027401][T183] nvme nvme0: creating 2 I/O queues. [5.029017][T183] nvme nvme0: mapped 2/0/0 default/read/poll queues. [5.032587][T183] nvme nvme0: new ctrl: NQN "nqn.2025-06.org.nvmexpress.mptcp", addr 127.0.0.1:4420, hostnqn: nqn.2014-08.org.nvmexpress:uuid:f7f6b5e0-ff97-4894-98ac-c85309e0bc77 [5.042214][T25] [5.042440][T25] ============================== [5.042579][T25] WARNING: suspicious RCU usage [5.042705][T25] 6.16.0-rc3+ #23 Not tainted [5.042812][T25] ----------------------------- [5.042934][T25] drivers/nvme/host/multipath.c:1203 RCU-list traversed in non-reader section!! [5.043111][T25] [5.043111][T25] other info that might help us debug this: [5.043111][T25] [5.043341][T25] [5.043341][T25] rcu_scheduler_active = 2, debug_locks = 1 [5.043502][T25] 3 locks held by kworker/u9:0/25: [5.043615][T25] #0: ffff888008730948 ((wq_completion)async){+.+.}-{0:0}, at: process_one_work+0x7ed/0x1350 [5.043830][T25] #1: ffffc900001afd40 ((work_completion)(&entry->work)){+.+.}-{0:0}, at: process_one_work+0xcf3/0x1350 [5.044084][T25] #2: ffff888013ee0020 (&head->srcu){.+.+}-{0:0}, at: nvme_mpath_add_sysfs_link.part.0+0xb4/0x3a0 [5.044300][T25] [5.044300][T25] stack backtrace: [5.044439][T25] CPU: 0 UID: 0 PID: 25 Comm: kworker/u9:0 Not tainted 6.16.0-rc3+ #23 PREEMPT(full) [5.044441][T25] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [5.044442][T25] Workqueue: async async_run_entry_fn [5.044445][T25] Call Trace: [5.044446][T25] <TASK> [5.044449][T25] dump_stack_lvl+0x6f/0xb0 [5.044453][T25] lockdep_rcu_suspicious.cold+0x4f/0xb1 [5.044457][T25] nvme_mpath_add_sysfs_link.part.0+0x2fb/0x3a0 [5.044459][T25] ? queue_work_on+0x90/0xf0 [5.044461][T25] ? lockdep_hardirqs_on+0x78/0x110 [5.044466][T25] nvme_mpath_set_live+0x1e9/0x4f0 [5.044470][T25] nvme_mpath_add_disk+0x240/0x2f0 [5.044472][T25] ? __pfx_nvme_mpath_add_disk+0x10/0x10 [5.044475][T25] ? add_disk_fwnode+0x361/0x580 [5.044480][T25] nvme_alloc_ns+0x81c/0x17c0 [5.044483][T25] ? kasan_quarantine_put+0x104/0x240 [5.044487][T25] ? __pfx_nvme_alloc_ns+0x10/0x10 [5.044495][T25] ? __pfx_nvme_find_get_ns+0x10/0x10 [5.044496][T25] ? rcu_read_lock_any_held+0x45/0xa0 [5.044498][T25] ? validate_chain+0x232/0x4f0 [5.044503][T25] nvme_scan_ns+0x4c8/0x810 [5.044506][T25] ? __pfx_nvme_scan_ns+0x10/0x10 [5.044508][T25] ? find_held_lock+0x2b/0x80 [5.044512][T25] ? ktime_get+0x16d/0x220 [5.044517][T25] ? kvm_clock_get_cycles+0x18/0x30 [5.044520][T25] ? __pfx_nvme_scan_ns_async+0x10/0x10 [5.044522][T25] async_run_entry_fn+0x97/0x560 [5.044523][T25] ? rcu_is_watching+0x12/0xc0 [5.044526][T25] process_one_work+0xd3c/0x1350 [5.044532][T25] ? __pfx_process_one_work+0x10/0x10 [5.044536][T25] ? assign_work+0x16c/0x240 [5.044539][T25] worker_thread+0x4da/0xd50 [5.044545][T25] ? __pfx_worker_thread+0x10/0x10 [5.044546][T25] kthread+0x356/0x5c0 [5.044548][T25] ? __pfx_kthread+0x10/0x10 [5.044549][T25] ? ret_from_fork+0x1b/0x2e0 [5.044552][T25] ? __lock_release.isra.0+0x5d/0x180 [5.044553][T25] ? ret_from_fork+0x1b/0x2e0 [5.044555][T25] ? rcu_is_watching+0x12/0xc0 [5.044557][T25] ? __pfx_kthread+0x10/0x10 [5.04 ---truncated---	N/A	More Details
CVE-2025-38396	In the Linux kernel, the following vulnerability has been resolved: fs: export anon_inode_make_secure_inode() and fix secretmem LSM bypass Export anon_inode_make_secure_inode() to allow KVM guest_memfd to create anonymous inodes with proper security context. This replaces the current pattern of calling alloc_anon_inode() followed by inode_init_security_anon() for creating security context manually. This change also fixes a security regression in secretmem where the S_PRIVATE flag was not cleared after alloc_anon_inode(), causing LSM/SELinux checks to be bypassed for secretmem file descriptors. As guest_memfd currently resides in the KVM module, we need to export this symbol for use outside the core kernel. In the future, guest_memfd might be moved to core-mm, at which point the symbols no longer would have to be exported. When/if that happens is still unclear.	N/A	More Details
CVE-2025-38395	In the Linux kernel, the following vulnerability has been resolved: regulator: gpio: Fix the out-of-bounds access to drvdata::gpiods drvdata::gpiods is supposed to hold an array of 'gpio_desc' pointers. But the memory is allocated for only one pointer. This will lead to out-of-bounds access later in the code if 'config::ngpios' is > 1. So fix the code to allocate enough memory to hold 'config::ngpios' of GPIO descriptors. While at it, also move the check for memory allocation failure to be below the allocation to make it more readable.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: HID: appletb-kbd: fix memory corruption of input_handler_list In appletb_kbd_probe an input handler is initialised and then registered with input core through input_register_handler(). When this happens input core will add the input handler (specifically its node) to the global input_handler_list. The input_handler_list		

CVE-2025-38394	is central to the functionality of input core and is traversed in various places in input core. An example of this is when a new input device is plugged in and gets registered with input core. The input_handler in probe is allocated as device managed memory. If a probe failure occurs after input_register_handler() the input_handler memory is freed, yet it will remain in the input_handler_list. This effectively means the input_handler_list contains a dangling pointer to data belonging to a freed input handler. This causes an issue when any other input device is plugged in - in my case I had an old PixArt HP USB optical mouse and I decided to plug it in after a failure occurred after input_register_handler(). This lead to the registration of this input device via input_register_device which involves traversing over every handler in the corrupted input_handler_list and calling input_attach_handler(), giving each handler a chance to bind to newly registered device. The core of this bug is a UAF which causes memory corruption of input_handler_list and to fix it we must ensure the input handler is unregistered from input core, this is done through input_unregister_handler(). [63.191597] == [63.192094] BUG: KASAN: slab-use-after-free in input_attach_handler.isra.0+0x1a9/0x1e0 [63.192094] Read of size 8 at addr ffff888105ea7c80 by task kworker/0:2/54 [63.192094] [63.192094] CPU: 0 UID: 0 PID: 54 Comm: kworker/0:2 Not tainted 6.16.0-rc2-00321-g2aa6621d [63.192094] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.164 [63.192094] Workqueue: usb_hub_wq hub_event [63.192094] Call Trace: [63.192094] <TASK> [63.192094] dump_stack_lvl+0x53/0x70 [63.192094] print_report+0xce/0x670 [63.192094] kasan_report+0xce/0x100 [63.192094] input_attach_handler.isra.0+0x1a9/0x1e0 [63.192094] input_register_device+0x76c/0xd00 [63.192094] hidinput_connect+0x686d/0xad60 [63.192094] hid_connect+0xf20/0x1b10 [63.192094] hid_hw_start+0x83/0x100 [63.192094] hid_device_probe+0x2d1/0x680 [63.192094] really_probe+0x1c3/0x690 [63.192094] __driver_probe_device+0x247/0x300 [63.192094] driver_probe_device+0x49/0x210 [63.192094] __device_attach_driver+0x160/0x320 [63.192094] bus_for_each_drv+0x10f/0x190 [63.192094] __device_attach+0x18e/0x370 [63.192094] bus_probe_device+0x123/0x170 [63.192094] device_add+0xd4d/0x1460 [63.192094] hid_add_device+0x30b/0x910 [63.192094] usbhid_probe+0x920/0xe00 [63.192094] usb_probe_interface+0x363/0x9a0 [63.192094] really_probe+0x1c3/0x690 [63.192094] __driver_probe_device+0x247/0x300 [63.192094] driver_probe_device+0x49/0x210 [63.192094] __device_attach_driver+0x160/0x320 [63.192094] bus_for_each_drv+0x10f/0x190 [63.192094] __device_attach+0x18e/0x370 [63.192094] bus_probe_device+0x123/0x170 [63.192094] device_add+0xd4d/0x1460 [63.192094] usb_set_configuration+0xd14/0x1880 [63.192094] usb_generic_driver_probe+0x78/0xb0 [63.192094] usb_probe_device+0xaa/0x2e0 [63.192094] really_probe+0x1c3/0x690 [63.192094] __driver_probe_device+0x247/0x300 [63.192094] driver_probe_device+0x49/0x210 [63.192094] __device_attach_driver+0x160/0x320 [63.192094] bus_for_each_drv+0x10f/0x190 [63.192094] __device_attach+0x18e/0x370 [63.192094] bus_probe_device+0x123/0x170 [63.192094] device_add+0xd4d/0x1460 [63.192094] usb_new_device+0x7b4/0x1000 [63.192094] hub_event+0x234d/0x3 ---truncated---	N/A	More Details
CVE-2025-38393	In the Linux kernel, the following vulnerability has been resolved: NFSv4/pNFS: Fix a race to wake on NFS_LAYOUT_DRAIN We found a few different systems hung up in writeback waiting on the same page lock, and one task waiting on the NFS_LAYOUT_DRAIN bit in pnfs_update_layout(), however the pnfs_layout_hdr's plh_outstanding count was zero. It seems most likely that this is another race between the waiter and waker similar to commit ed0172af5d6f ("SUNRPC: Fix a race to wake a sync task"). Fix it up by applying the advised barrier.	N/A	More Details
CVE-2025-38392	In the Linux kernel, the following vulnerability has been resolved: idpf: convert control queue mutex to a spinlock With VIRTCHNL2_CAP_MACFILTER enabled, the following warning is generated on module load: [324.701677] BUG: sleeping function called from invalid context at kernel/locking/mutex.c:578 [324.701684] in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 1582, name: NetworkManager [324.701689] preempt_count: 201, expected: 0 [324.701693] RCU nest depth: 0, expected: 0 [324.701697] 2 locks held by NetworkManager/1582: [324.701702] #0: ffffffff9f7be770 (rtnl_mutex){....}-{3:3}, at: rtnl_newlink+0x791/0x21e0 [324.701730] #1: ff1100216c380368 (_xmit_ETHER){....}-{2:2}, at: __dev_open+0x3f0/0x870 [324.701749] Preemption disabled at: [324.701752] [<ffffffff9cd23b9d>] __dev_open+0x3dd/0x870 [324.701765] CPU: 30 UID: 0 PID: 1582 Comm: NetworkManager Not tainted 6.15.0-rc5+ #2 PREEMPT(voluntary) [324.701771] Hardware name: Intel Corporation M50FCP2SBSTD/M50FCP2SBSTD, BIOS SE5C741.86B.01.01.0001.2211140926 11/14/2022 [324.701774] Call Trace: [324.701777] <TASK> [324.701779] dump_stack_lvl+0x5d/0x80 [324.701788] ? __dev_open+0x3dd/0x870 [324.701793] __might_resched.cold+0x1ef/0x23d <..> [324.701818] __mutex_lock+0x113/0x1b80 <..> [324.701917] idpf_ctlq_clean_sq+0xad/0x4b0 [idpf] [324.701935] ? kasan_save_track+0x14/0x30 [324.701941] idpf_mb_clean+0x143/0x380 [idpf] <..> [324.701991] idpf_send_mb_msg+0x111/0x720 [idpf] [324.702009] idpf_vc_xn_exec+0x4cc/0x990 [idpf] [324.702021] ? rcu_is_watching+0x12/0xc0 [324.702035] idpf_add_del_mac_filters+0x3ed/0xb50 [idpf] <..> [324.702122] __hw_addr_sync_dev+0x1cf/0x300 [324.702126] ? find_held_lock+0x32/0x90 [324.702134] idpf_set_rx_mode+0x317/0x390 [idpf] [324.702152] __dev_open+0x3f8/0x870 [324.702159] ? __pfx___dev_open+0x10/0x10 [324.702174] __dev_change_flags+0x443/0x650 <..> [324.702208] netif_change_flags+0x80/0x160 [324.702218] do_setlink.isra.0+0x16a0/0x3960 <..> [324.702349] rtnl_newlink+0x12fd/0x21e0 The sequence is as follows: rtnl_newlink()-> __dev_change_flags()-> __dev_open()-> dev_set_rx_mode() - > # disables BH and grabs "dev->addr_list_lock" idpf_set_rx_mode() -> # proceed only if VIRTCHNL2_CAP_MACFILTER is ON __dev_uc_sync() -> idpf_add_mac_filter -> idpf_add_del_mac_filters -> idpf_send_mb_msg() -> idpf_mb_clean() -> idpf_ctlq_clean_sq() # mutex_lock(cq_lock) Fix by converting cq_lock to a spinlock. All operations under the new lock are safe except freeing the DMA memory, which may use vunmap(). Fix by requesting a contiguous physical memory for the DMA mapping.	N/A	More Details
CVE-2025-38391	In the Linux kernel, the following vulnerability has been resolved: usb: typec: altmodes/displayport: do not index invalid pin_assignments A poorly implemented DisplayPort Alt Mode port partner can indicate that its pin assignment capabilities are greater than the maximum value, DP_PIN_ASSIGN_F. In this case, calls to pin_assignment_show will cause a BRK exception due to an out of bounds array access. Prevent for loop in pin_assignment_show from accessing invalid values in pin_assignments by adding DP_PIN_ASSIGN_MAX value in typec_dp.h and using i < DP_PIN_ASSIGN_MAX as a loop condition.	N/A	More Details
CVE-2025-38390	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_ffa: Fix memory leak by freeing notifier callback node Commit e0573444edbf ("firmware: arm_ffa: Add interfaces to request notification callbacks") adds support for notifier callbacks by allocating and inserting a callback node into a hashtable during registration of notifiers. However, during unregistration, the code only removes the node from the hashtable without freeing the associated memory, resulting in a memory leak. Resolve the memory leak issue by ensuring the allocated notifier callback node is properly freed after it is removed from the hashtable entry.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Fix timeline left held on VMA alloc error The following error has been reported sporadically by CI when a test unbinds the i915 driver on a ring submission platform: <4> [239.330153] ------------[cut here]------------ <4> [239.330166] i915 0000:00:02.0: [drm] drm_WARN_ON(dev_priv-		

CVE-2025-38389	>mm.shrink_count) <4> [239.330196] WARNING: CPU: 1 PID: 18570 at drivers/gpu/drm/i915/i915_gem.c:1309 i915_gem_cleanup_early+0x13e/0x150 [i915] ... <4> [239.330640] RIP: 0010:i915_gem_cleanup_early+0x13e/0x150 [i915] ... <4> [239.330942] Call Trace: <4> [239.330944] <TASK> <4> [239.330949] i915_driver_late_release+0x2b/0xa0 [i915] <4> [239.331202] i915_driver_release+0x86/0xa0 [i915] <4> [239.331482] devm_drm_dev_init_release+0x61/0x90 <4> [239.331494] devm_action_release+0x15/0x30 <4> [239.331504] release_nodes+0x3d/0x120 <4> [239.331517] devres_release_all+0x96/0xd0 <4> [239.331533] device_unbind_cleanup+0x12/0x80 <4> [239.331543] device_release_driver_internal+0x23a/0x280 <4> [239.331550] ? bus_find_device+0xa5/0xe0 <4> [239.331563] device_driver_detach+0x14/0x20 ... <4> [357.719679] ---[end trace 0000000000000000]--- If the test also unloads the i915 module then that's followed with: <3> [357.787478] === <3> [357.788006] BUG i915_vma (Tainted: G U W N): Objects remaining on __kmem_cache_shutdown() <3> [357.788031] --- <3> [357.788204] Object 0xffff888109e7f480 @offset=29824 <3> [357.788670] Allocated in i915_vma_instance+0xee/0xc10 [i915] age=292729 cpu=4 pid=2244 <4> [357.788994] i915_vma_instance+0xee/0xc10 [i915] <4> [357.789290] init_status_page+0x7b/0x420 [i915] <4> [357.789532] intel_engines_init+0x1d8/0x980 [i915] <4> [357.789772] intel_gt_init+0x175/0x450 [i915] <4> [357.790014] i915_gem_init+0x113/0x340 [i915] <4> [357.790281] i915_driver_probe+0x847/0xed0 [i915] <4> [357.790504] i915_pci_probe+0xe6/0x220 [i915] ... Closer analysis of CI results history has revealed a dependency of the error on a few IGT tests, namely: - igt@api_intel_allocator@fork-simple-stress-signal, - igt@api_intel_allocator@two-level-inception-interruptible, - igt@gem_linear_blits@interruptible, - igt@prime_mmap_coherency@ioctl-errors, which invisibly trigger the issue, then exhibited with first driver unbind attempt. All of the above tests perform actions which are actively interrupted with signals. Further debugging has allowed to narrow that scope down to DRM_IOCTL_I915_GEM_EXECBUFFER2, and ring_context_alloc(), specific to ring submission, in particular. If successful then that function, or its execlists or GuC submission equivalent, is supposed to be called only once per GEM context engine, followed by raise of a flag that prevents the function from being called again. The function is expected to unwind its internal errors itself, so it may be safely called once more after it returns an error. In case of ring submission, the function first gets a reference to the engine's legacy timeline and then allocates a VMA. If the VMA allocation fails, e.g. when i915_vma_instance() called from inside is interrupted with a signal, then ring_context_alloc() fails, leaving the timeline held referenced. On next I915_GEM_EXECBUFFER2 IOCTL, another reference to the timeline is got, and only that last one is put on successful completion. As a consequence, the legacy timeline, with its underlying engine status page's VMA object, is still held and not released on driver unbind. Get the legacy timeline only after successful allocation of the context engine's VMA. v2: Add a note on other submission methods (Krzysztof Karas): Both execlists and GuC submission use lrc_alloc() which seems free from a similar issue. (cherry picked from commit cc43422b3cc79eacff4c5a8ba0d224688ca9dd4f)	N/A	More Details
CVE-2025-38388	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_ffa: Replace mutex with rwlock to avoid sleep in atomic context The current use of a mutex to protect the notifier hashtable accesses can lead to issues in the atomic context. It results in the below kernel warnings: | BUG: sleeping function called from invalid context at kernel/locking/mutex.c:258 | in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 9, name: kworker/0:0 | preempt_count: 1, expected: 0 | RCU nest depth: 0, expected: 0 | CPU: 0 UID: 0 PID: 9 Comm: kworker/0:0 Not tainted 6.14.0 #4 | Workqueue: ffa_pcpu_irq_notification notif_pcpu_irq_work_fn | Call trace: | show_stack+0x18/0x24 (C) | dump_stack_lvl+0x78/0x90 | dump_stack+0x18/0x24 | __might_resched+0x114/0x170 | __might_sleep+0x48/0x98 | mutex_lock+0x24/0x80 | handle_notif_callbacks+0x54/0xe0 | notif_get_and_handle+0x40/0x88 | generic_exec_single+0x80/0xc0 | smp_call_function_single+0xfc/0x1a0 | notif_pcpu_irq_work_fn+0x2c/0x38 | process_one_work+0x14c/0x2b4 | worker_thread+0x2e4/0x3e0 | kthread+0x13c/0x210 | ret_from_fork+0x10/0x20 To address this, replace the mutex with an rwlock to protect the notifier hashtable accesses. This ensures that read-side locking does not sleep and multiple readers can acquire the lock concurrently, avoiding unnecessary contention and potential deadlocks. Writer access remains exclusive, preserving correctness. This change resolves warnings from lockdep about potential sleep in atomic context.	N/A	More Details
CVE-2025-38387	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Initialize obj_event->obj_sub_list before xa_insert The obj_event may be loaded immediately after inserted, then if the list_head is not initialized then we may get a poisonous pointer. This fixes the crash below: mlx5_core 0000:03:00.0: MLX5E: StrdRq(1) RqSz(8) StrdSz(2048) RxCqeCmprss(0 enhanced) mlx5_core.sf mlx5_core.sf.4: firmware version: 32.38.3056 mlx5_core 0000:03:00.0 en3f0pf0sf2002: renamed from eth0 mlx5_core.sf mlx5_core.sf.4: Rate limit: 127 rates are supported, range: 0Mbps to 195312Mbps IPv6: ADDRCONF(NETDEV_CHANGE): en3f0pf0sf2002: link becomes ready Unable to handle kernel NULL pointer dereference at virtual address 0000000000000060 Mem abort info: ESR = 0x96000006 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 Data abort info: ISV = 0, ISS = 0x00000006 CM = 0, WnR = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=00000007760fb000 [0000000000000060] pgd=000000076f6d7003, p4d=000000076f6d7003, pud=0000000777841003, pmd=0000000000000000 Internal error: Oops: 96000006 [#1] SMP Modules linked in: ipmb_host(OE) act_mirred(E) cls_flower(E) sch_ingress(E) mptcp_diag(E) udp_diag(E) raw_diag(E) unix_diag(E) tcp_diag(E) inet_diag(E) binfmt_misc(E) bonding(OE) rdma_ucm(OE) rdma_cm(OE) iw_cm(OE) ib_ipoib(OE) ib_cm(OE) isofs(E) cdrom(E) mst_pciconf(OE) ib_umad(OE) mlx5_ib(OE) ipmb_dev_int(OE) mlx5_core(OE) kpatch_15237886(OEK) mlxdevm(OE) auxiliary(OE) ib_uverbs(OE) ib_core(OE) psample(E) mlxfw(OE) tls(E) sunrpc(E) vfat(E) fat(E) crct10dif_ce(E) ghash_ce(E) sha1_ce(E) sbsa_gwdt(E) virtio_console(E) ext4(E) mbcache(E) jbd2(E) xfs(E) libcrc32c(E) mmc_block(E) virtio_net(E) net_failover(E) failover(E) sha2_ce(E) sha256_arm64(E) nvme(OE) nvme_core(OE) gpio_mlxbf3(OE) mlx_compat(OE) mlxbf_pmc(OE) i2c_mlxbf(OE) sdhci_of_dwcmshc(OE) pinctrl_mlxbf3(OE) mlxbf_pka(OE) gpio_generic(E) i2c_core(E) mmc_core(E) mlxbf_gige(OE) vitesse(E) pwr_mlxbf(OE) mlxbf_tmfifo(OE) micrel(E) mlxbf_bootctl(OE) virtio_ring(E) virtio(E) ipmi_devintf(E) ipmi_msghandler(E) [last unloaded: mst_pci] CPU: 11 PID: 20913 Comm: rte-worker-11 Kdump: loaded Tainted: G OE K 5.10.134-13.1.an8.aarch64 #1 Hardware name: https://www.mellanox.com BlueField-3 SmartNIC Main Card/BlueField-3 SmartNIC Main Card, BIOS 4.2.2.12968 Oct 26 2023 pstate: a0400089 (NzCv daIf +PAN -UAO -TCO BTYPE=--) pc : dispatch_event_fd+0x68/0x300 [mlx5_ib] lr : devx_event_notifier+0xcc/0x228 [mlx5_ib] sp : ffff80001005bcf0 x29: ffff80001005bcf0 x28: 0000000000000001 x27: ffff244e0740a1d8 x26: ffff244e0740a1d0 x25: ffffda56beff5ae0 x24: ffffda56bf911618 x23: ffff244e0596a480 x22: ffff244e0596a480 x21: ffff244d8312ad90 x20: ffff244e0596a480 x19: fffffffffffffff0 x18: 0000000000000000 x17: 0000000000000000 x16: ffffda56be66d620 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000040 x10: ffffda56bfcafb50 x9 : ffffda5655c25f2c x8 : 0000000000000010 x7 : 0000000000000000 x6 : ffff24545a2e24b8 x5 : 0000000000000003 x4 : ffff80001005bd28 x3 : 0000000000000000 x2 : 0000000000000000 x1 : ffff244e0596a480 x0 : ffff244d8312ad90 Call trace: dispatch_event_fd+0x68/0x300 [mlx5_ib] devx_event_notifier+0xcc/0x228 [mlx5_ib] atomic_notifier_call_chain+0x58/0x80 mlx5_eq_async_int+0x148/0x2b0 [mlx5_core] atomic_notifier_call_chain+0x58/0x80 irq_int_handler+0x20/0x30 [mlx5_core] __handle_irq_event_percpu+0x60/0x220 handle_irq_event_percpu+0x3c/0x90 handle_irq_event+0x58/0x158 handle_fasteoi_irq+0xfc/0x188 generic_handle_irq+0x34/0x48 ...	N/A	More Details

CVE-2025-38386	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Refuse to evaluate a method if arguments are missing As reported in [1], a platform firmware update that increased the number of method parameters and forgot to update a least one of its callers, caused ACPICA to crash due to use-after-free. Since this a result of a clear AML issue that arguably cannot be fixed up by the interpreter (it cannot produce missing data out of thin air), address it by making ACPICA refuse to evaluate a method if the caller attempts to pass fewer arguments than expected to it.	N/A	More Details
CVE-2025-38405	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix memory leak of bio integrity If nvmet receives commands with metadata there is a continuous memory leak of kmalloc-128 slab or more precisely bio->bi_integrity. Since commit bf4c89fc8797 ("block: don't call bio_uninit from bio_endio") each user of bio_init has to use bio_uninit as well. Otherwise the bio integrity is not getting free. Nvmet uses bio_init for inline bios. Uninit the inline bio to complete deallocation of integrity in bio.	N/A	More Details
CVE-2025-38406	In the Linux kernel, the following vulnerability has been resolved: wifi: ath6kl: remove WARN on bad firmware input If the firmware gives bad input, that's nothing to do with the driver's stack at this point etc., so the WARN_ON() doesn't add any value. Additionally, this is one of the top syzbot reports now. Just print a message, and as an added bonus, print the sizes too.	N/A	More Details
CVE-2025-38407	In the Linux kernel, the following vulnerability has been resolved: riscv: cpu_ops_sbi: Use static array for boot_data Since commit 6b9f29b81b15 ("riscv: Enable pcpu page first chunk allocator"), if NUMA is enabled, the page percpu allocator may be used on very sparse configurations, or when requested on boot with percpu_alloc=page. In that case, percpu data gets put in the vmalloc area. However, sbi_hsm_hart_start() needs the physical address of a sbi_hart_boot_data, and simply assumes that __pa() would work. This causes the just started hart to immediately access an invalid address and hang. Fortunately, struct sbi_hart_boot_data is not too large, so we can simply allocate an array for boot_data statically, putting it in the kernel image. This fixes NUMA=y SMP boot on Sophgo SG2042. To reproduce on QEMU: Set CONFIG_NUMA=y and CONFIG_DEBUG_VIRTUAL=y, then run with: qemu-system-riscv64 -M virt -smp 2 -nographic \ -kernel arch/riscv/boot/Image \ -append "percpu_alloc=page" Kernel output: [0.000000] Booting Linux on hartid 0 [0.000000] Linux version 6.16.0-rc1 (dram@sakuya) (riscv64-unknown-linux-gnu-gcc (GCC) 14.2.1 20250322, GNU ld (GNU Binutils) 2.44) #11 SMP Tue Jun 24 14:56:22 CST 2025 ... [0.000000] percpu: 28 4K pages/cpu s85784 r8192 d20712 ... [0.083192] smp: Bringing up secondary CPUs ... [0.086722] ------------[cut here]------------ [0.086849] virt_to_phys used for non-linear address: (____ptrval____) (0xff2000000001d080) [0.088001] WARNING: CPU: 0 PID: 1 at arch/riscv/mm/physaddr.c:14 __virt_to_phys+0xae/0xe8 [0.088376] Modules linked in: [0.088656] CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.16.0-rc1 #11 NONE [0.088833] Hardware name: riscv-virtio,qemu (DT) [0.088948] epc : __virt_to_phys+0xae/0xe8 [0.089001] ra : __virt_to_phys+0xae/0xe8 [0.089037] epc : ffffffff80021eaa ra : ffffffff80021eaa sp : ff2000000004bbc0 [0.089057] gp : ffffffff817f49c0 tp : ff60000001d60000 t0 : 5f6f745f74726976 [0.089076] t1 : 0000000000000076 t2 : 705f6f745f747269 s0 : ff2000000004bbe0 [0.089095] s1 : ff2000000001d080 a0 : 0000000000000000 a1 : 0000000000000000 [0.089113] a2 : 0000000000000000 a3 : 0000000000000000 a4 : 0000000000000000 [0.089131] a5 : 0000000000000000 a6 : 0000000000000000 a7 : 0000000000000000 [0.089155] s2 : ffffffff8130dc00 s3 : 0000000000000001 s4 : 0000000000000001 [0.089174] s5 : ffffffff8185eff8 s6 : ff2000007f1eb000 s7 : ffffffff8002a2ec [0.089193] s8 : 0000000000000001 s9 : 0000000000000001 s10: 0000000000000000 [0.089211] s11: 0000000000000000 t3 : ffffffff8180a9f7 t4 : ffffffff8180a9f7 [0.089960] t5 : ffffffff8180a9f8 t6 : ff2000000004b9d8 [0.089984] status: 0000000200000120 badaddr: ffffffff80021eaa cause: 0000000000000003 [0.090101] [<ffffffff80021eaa>] __virt_to_phys+0xae/0xe8 [0.090228] [<ffffffff8001d796>] sbi_cpu_start+0x6e/0xe8 [0.090247] [<ffffffff8001a5da>] __cpu_up+0x1e/0x8c [0.090260] [<ffffffff8002a32e>] bringup_cpu+0x42/0x258 [0.090277] [<ffffffff8002914c>] cpuhp_invoke_callback+0xe0/0x40c [0.090292] [<ffffffff800294e0>] __cpuhp_invoke_callback_range+0x68/0xfc [0.090320] [<ffffffff8002a96a>] _cpu_up+0x11a/0x244 [0.090334] [<ffffffff8002aae6>] cpu_up+0x52/0x90 [0.090384] [<ffffffff80c09350>] bringup_nonboot_cpus+0x78/0x118 [0.090411] [<ffffffff80c11060>] smp_init+0x34/0xb8 [0.090425] [<ffffffff80c01220>] kernel_init_freeable+0x148/0x2e4 [0.090442] [<ffffffff80b83802>] kernel_init+0x1e/0x14c [0.090455] [<ffffffff800124ca>] ret_from_fork_kernel+0xe/0xf0 [0.090471] [<ffffffff80b8d9c2>] ret_from_fork_kernel_asm+0x16/0x18 [0.090560] ---[end trace 0000000000000000]--- [1.179875] CPU1: failed to come online [1.190324] smp: Brought up 1 node, 1 CPU	N/A	More Details
CVE-2025-38418	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Release rproc->clean_table after rproc_attach() fails When rproc->state = RPROC_DETACHED is attached to remote processor through rproc_attach(), if rproc_handle_resources() returns failure, then the clean table should be released, otherwise the following memory leak will occur. unreferenced object 0xffff000086a99800 (size 1024): comm "kworker/u12:3", pid 59, jiffies 4294893670 (age 121.140s) hex dump (first 32 bytes): 00 00 00 00 00 80 00 00 00 00 00 00 00 00 10 00 .... 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 .... backtrace: [<000000008bbe4ca8>] slab_post_alloc_hook+0x98/0x3fc [<000000003b8a272b>] __kmem_cache_alloc_node+0x13c/0x230 [<000000007a507c51>] __kmalloc_node_track_caller+0x5c/0x260 [<0000000037818dae>] kmemdup+0x34/0x60 [<00000000610f7f57>] rproc_boot+0x35c/0x56c [<0000000065f8871a>] rproc_add+0x124/0x17c [<00000000497416ee>] imx_rproc_probe+0x4ec/0x5d4 [<000000003bcaa37d>] platform_probe+0x68/0xd8 [<00000000771577f9>] really_probe+0x110/0x27c [<00000000531fea59>] __driver_probe_device+0x78/0x12c [<0000000080036a04>] driver_probe_device+0x3c/0x118 [<000000007e0bddcb>] __device_attach_driver+0xb8/0xf8 [<000000000cf1fa33>] bus_for_each_drv+0x84/0xe4 [<000000001a53b53e>] __device_attach+0xfc/0x18c [<00000000d1a2a32c>] device_initial_probe+0x14/0x20 [<00000000d8f8b7ae>] bus_probe_device+0xb0/0xb4 unreferenced object 0xffff0000864c9690 (size 16):	N/A	More Details
CVE-2025-38426	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Add basic validation for RAS header If RAS header read from EEPROM is corrupted, it could result in trying to allocate huge memory for reading the records. Add some validation to header fields.	N/A	More Details
CVE-2025-38425	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: check msg length in SMBUS block read For SMBUS block read, do not continue to read if the message length passed from the device is '0' or greater than the maximum allowed bytes.	N/A	More Details
CVE-2025-38424	In the Linux kernel, the following vulnerability has been resolved: perf: Fix sample vs do_exit() Baisheng Gao reported an ARM64 crash, which Mark decoded as being a synchronous external abort -- most likely due to trying to access MMIO in bad ways. The crash further shows perf trying to do a user stack sample while in exit_mmap()'s tlb_finish_mmu() -- i.e. while tearing down the address space it is trying to access. It turns out that we stop perf after we tear down the userspace mm; a receipie for disaster, since perf likes to access userspace for various reasons. Flip this order by moving up where we stop perf in do_exit(). Additionally, harden PERF_SAMPLE_CALLCHAIN and PERF_SAMPLE_STACK_USER to abort when the current task does not have an mm (exit_mm() makes sure to set current->mm = NULL; before commencing with the actual teardown). Such that CPU wide	N/A	More Details

	events don't trip on this same problem.		
CVE-2025-38423	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: wcd9375: Fix double free of regulator supplies Driver gets regulator supplies in probe path with devm_regulator_bulk_get(), so should not call regulator_bulk_free() in error and remove paths to avoid double free.	N/A	More Details
CVE-2025-38422	In the Linux kernel, the following vulnerability has been resolved: net: lan743x: Modify the EEPROM and OTP size for PCI1xxxx devices Maximum OTP and EEPROM size for hearthstone PCI1xxxx devices are 8 Kb and 64 Kb respectively. Adjust max size definitions and return correct EEPROM length based on device. Also prevent out-of-bound read/write.	N/A	More Details
CVE-2025-38421	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd: pmf: Use device managed allocations If setting up smart PC fails for any reason then this can lead to a double free when unloading amd-pmf. This is because dev->buf was freed but never set to NULL and is again freed in amd_pmf_remove(). To avoid subtle allocation bugs in failures leading to a double free change all allocations into device managed allocations.	N/A	More Details
CVE-2025-38420	In the Linux kernel, the following vulnerability has been resolved: wifi: carl9170: do not ping device which has failed to load firmware Syzkaller reports [1, 2] crashes caused by an attempts to ping the device which has failed to load firmware. Since such a device doesn't pass 'ieee80211_register_hw()', an internal workqueue managed by 'ieee80211_queue_work()' is not yet created and an attempt to queue work on it causes null-ptr-deref. [1] https://syzkaller.appspot.com/bug?extid=9a4aec827829942045ff [2] https://syzkaller.appspot.com/bug?extid=0d8afba53e8fb2633217	N/A	More Details
CVE-2025-38419	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Cleanup acquired resources when rproc_handle_resources() fails in rproc_attach() When rproc->state = RPROC_DETACHED and rproc_attach() is used to attach to the remote processor, if rproc_handle_resources() returns a failure, the resources allocated by imx_rproc_prepare() should be released, otherwise the following memory leak will occur. Since almost the same thing is done in imx_rproc_prepare() and rproc_resource_cleanup(), Function rproc_resource_cleanup() is able to deal with empty lists so it is better to fix the "goto" statements in rproc_attach(). replace the "unprepare_device" goto statement with "clean_up_resources" and get rid of the "unprepare_device" label. unreferenced object 0xffff0000861c5d00 (size 128): comm "kworker/u12:3", pid 59, jiffies 4294893509 (age 149.220s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 00 00 02 88 00 00 00 00 00 00 10 00 00 00 00 00 .... backtrace: [<00000000f949fe18>] slab_post_alloc_hook+0x98/0x37c [<00000000adbfb3e7>] __kmem_cache_alloc_node+0x138/0x2e0 [<00000000521c0345>] kmalloc_trace+0x40/0x158 [<000000004e330a49>] rproc_mem_entry_init+0x60/0xf8 [<000000002815755e>] imx_rproc_prepare+0xe0/0x180 [<0000000003f61b4e>] rproc_boot+0x2ec/0x528 [<00000000e7e994ac>] rproc_add+0x124/0x17c [<0000000048594076>] imx_rproc_probe+0x4ec/0x5d4 [<00000000efc298a1>] platform_probe+0x68/0xd8 [<00000000110be6fe>] really_probe+0x110/0x27c [<00000000e245c0ae>] __driver_probe_device+0x78/0x12c [<00000000f61f6f5e>] driver_probe_device+0x3c/0x118 [<00000000a7874938>] __device_attach_driver+0xb8/0xf8 [<0000000065319e69>] bus_for_each_drv+0x84/0xe4 [<00000000db3eb243>] __device_attach+0xfc/0x18c [<0000000072e4e1a4>] device_initial_probe+0x14/0x20	N/A	More Details
CVE-2025-38417	In the Linux kernel, the following vulnerability has been resolved: ice: fix eswitch code memory leak in reset scenario Add simple eswitch mode checker in attaching VF procedure and allocate required port representor memory structures only in switchdev mode. The reset flows triggers VF (if present) detach/attach procedure. It might involve VF port representor(s) re-creation if the device is configured is switchdev mode (not legacy one). The memory was blindly allocated in current implementation, regardless of the mode and not freed if in legacy mode. Kmemeleak trace: unreferenced object (percpu) 0x7e3bce5b888458 (size 40): comm "bash", pid 1784, jiffies 4295743894 hex dump (first 32 bytes on cpu 45): 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 (crc 0): pcpu_alloc_noprof+0x4c4/0x7c0 ice_repr_create+0x66/0x130 [ice] ice_repr_create_vf+0x22/0x70 [ice] ice_eswitch_attach_vf+0x1b/0xa0 [ice] ice_reset_all_vfs+0x1dd/0x2f0 [ice] ice_pci_err_resume+0x3b/0xb0 [ice] pci_reset_function+0x8f/0x120 reset_store+0x56/0xa0 kernfs_fop_write_iter+0x120/0x1b0 vfs_write+0x31c/0x430 ksys_write+0x61/0xd0 do_syscall_64+0x5b/0x180 entry_SYSCALL_64_after_hwframe+0x76/0x7e Testing hints (ethX is PF netdev): - create at least one VF echo 1 > /sys/class/net/ethX/device/sriov_numvfs - trigger the reset echo 1 > /sys/class/net/ethX/device/reset	N/A	More Details
CVE-2025-38408	In the Linux kernel, the following vulnerability has been resolved: genirq/irq_sim: Initialize work context pointers properly Initialize `ops` member's pointers properly by using kzalloc() instead of kmalloc() when allocating the simulation work context. Otherwise the pointers contain random content leading to invalid dereferencing.	N/A	More Details
CVE-2025-38416	In the Linux kernel, the following vulnerability has been resolved: NFC: nci: uart: Set tty->disc_data only in success path Setting tty->disc_data before opening the NCI device means we need to clean it up on error paths. This also opens some short window if device starts sending data, even before NCIUARTSETDRIVER IOCTL succeeded (broken hardware?). Close the window by exposing tty->disc_data only on the success path, when opening of the NCI device and try_module_get() succeeds. The code differs in error path in one aspect: tty->disc_data won't be ever assigned thus NULL-ified. This however should not be relevant difference, because of "tty->disc_data=NULL" in nci_uart_tty_open().	N/A	More Details
CVE-2025-38415	In the Linux kernel, the following vulnerability has been resolved: Squashfs: check return result of sb_min_blocksize Syzkaller reports an "UBSAN: shift-out-of-bounds in squashfs_bio_read" bug. Syzkaller forks multiple processes which after mounting the Squashfs filesystem, issues an ioctl("/dev/loop0", LOOP_SET_BLOCK_SIZE, 0x8000). Now if this ioctl occurs at the same time another process is in the process of mounting a Squashfs filesystem on /dev/loop0, the failure occurs. When this happens the following code in squashfs_fill_super() fails. ---- msblk->devblksize = sb_min_blocksize(sb, SQUASHFS_DEVBLK_SIZE); msblk->devblksize_log2 = ffz(~msblk->devblksize); ---- sb_min_blocksize() returns 0, which means msblk->devblksize is set to 0. As a result, ffz(~msblk->devblksize) returns 64, and msblk->devblksize_log2 is set to 64. This subsequently causes the UBSAN: shift-out-of-bounds in fs/squashfs/block.c:195:36 shift exponent 64 is too large for 64-bit type 'u64' (aka 'unsigned long long') This commit adds a check for a 0 return by sb_min_blocksize().	N/A	More Details
CVE-2025-38414	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix GCC_GCC_PCIE_HOT_RST definition for WCN7850 GCC_GCC_PCIE_HOT_RST is wrongly defined for WCN7850, causing kernel crash on some specific platforms. Since this register is divergent for WCN7850 and QCN9274, move it to register table to allow different definitions. Then correct the register address for WCN7850 to fix this issue. Note IPQ5332 is not affected as it is not PCIe based device. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.0.c5-00481-QCAHMTSWPL_V1.0_V2.0_SILICONZ-3	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: virtio-net: xsk: rx: fix the frame's length check When calling		

CVE-2025-38413	buf_to_xdp, the len argument is the frame data's length without virtio header's length (vi->hdr_len). We check that len with xsk_pool_get_rx_frame_size() + vi->hdr_len to ensure the provided len does not larger than the allocated chunk size. The additional vi->hdr_len is because in virtnet_add_recvbuf_xsk, we use part of XDP_PACKET_HEADROOM for virtio header and ask the vhost to start placing data from hard_start + XDP_PACKET_HEADROOM - vi->hdr_len not hard_start + XDP_PACKET_HEADROOM But the first buffer has virtio_header, so the maximum frame's length in the first buffer can only be xsk_pool_get_rx_frame_size() not xsk_pool_get_rx_frame_size() + vi->hdr_len like in the current check. This commit adds an additional argument to buf_to_xdp differentiate between the first buffer and other ones to correctly calculate the maximum frame's length.	N/A	More Details
CVE-2025-38412	In the Linux kernel, the following vulnerability has been resolved: platform/x86: dell-wmi-sysman: Fix WMI data block retrieval in sysfs callbacks After retrieving WMI data blocks in sysfs callbacks, check for the validity of them before dereferencing their content.	N/A	More Details
CVE-2025-38411	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix double put of request If a netfs request finishes during the pause loop, it will have the ref that belongs to the IN_PROGRESS flag removed at that point - however, if it then goes to the final wait loop, that will *also* put the ref because it sees that the IN_PROGRESS flag is clear and incorrectly assumes that this happened when it called the collector. In fact, since IN_PROGRESS is clear, we shouldn't call the collector again since it's done all the cleanup, such as calling ->ki_complete(). Fix this by making netfs_collect_in_app() just return, indicating that we're done if IN_PROGRESS is removed.	N/A	More Details
CVE-2025-38410	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix a fence leak in submit error path In error paths, we could unref the submit without calling drm_sched_entity_push_job(), so msm_job_free() will never get called. Since drm_sched_job_cleanup() will NULL out the s_fence, we can use that to detect this case. Patchwork: https://patchwork.freedesktop.org/patch/653584/	N/A	More Details
CVE-2025-38409	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix another leak in the submit error path put_unused_fd() doesn't free the installed file, if we've already done fd_install(). So we need to also free the sync_file. Patchwork: https://patchwork.freedesktop.org/patch/653583/	N/A	More Details
CVE-2025-38385	In the Linux kernel, the following vulnerability has been resolved: net: usb: lan78xx: fix WARN in __netif_napi_del_locked on disconnect Remove redundant netif_napi_del() call from disconnect path. A WARN may be triggered in __netif_napi_del_locked() during USB device disconnect: WARNING: CPU: 0 PID: 11 at net/core/dev.c:7417 __netif_napi_del_locked+0x2b4/0x350 This happens because netif_napi_del() is called in the disconnect path while NAPI is still enabled. However, it is not necessary to call netif_napi_del() explicitly, since unregister_netdev() will handle NAPI teardown automatically and safely. Removing the redundant call avoids triggering the warning. Full trace: lan78xx 1-1:1.0 enu1: Failed to read register index 0x000000c4. ret = -ENODEV lan78xx 1-1:1.0 enu1: Failed to set MAC down with error -ENODEV lan78xx 1-1:1.0 enu1: Link is Down lan78xx 1-1:1.0 enu1: Failed to read register index 0x00000120. ret = -ENODEV ------------[cut here]------------ WARNING: CPU: 0 PID: 11 at net/core/dev.c:7417 __netif_napi_del_locked+0x2b4/0x350 Modules linked in: flexcan can_dev fuse CPU: 0 UID: 0 PID: 11 Comm: kworker/0:1 Not tainted 6.16.0-rc2-00624-ge926949dab03 #9 PREEMPT Hardware name: SKOV IMX8MP CPU revC - bd500 (DT) Workqueue: usb_hub_wq hub_event pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __netif_napi_del_locked+0x2b4/0x350 lr : __netif_napi_del_locked+0x7c/0x350 sp : ffffffc085b673c0 x29: ffffffc085b673c0 x28: ffffff800b7f2000 x27: ffffff800b7f20d8 x26: ffffff80110bcf58 x25: ffffff80110bd978 x24: 1fffffff0022179eb x23: ffffff80110bc000 x22: ffffff800b7f5000 x21: ffffff80110bc000 x20: ffffff80110bcf38 x19: ffffff80110bcf28 x18: dfffffc000000000 x17: ffffffc081578940 x16: ffffffc08284cee0 x15: 0000000000000028 x14: 0000000000000006 x13: 0000000000040000 x12: ffffffb0022179e8 x11: 1fffffff0022179e7 x10: ffffffb0022179e7 x9 : dfffffc000000000 x8 : 0000004ffdde8619 x7 : ffffff80110bcf3f x6 : 0000000000000001 x5 : ffffff80110bcf38 x4 : ffffff80110bcf38 x3 : 0000000000000000 x2 : 0000000000000000 x1 : 1fffffff0022179e7 x0 : 0000000000000000 Call trace: __netif_napi_del_locked+0x2b4/0x350 (P) lan78xx_disconnect+0xf4/0x360 usb_unbind_interface+0x158/0x718 device_remove+0x100/0x150 device_release_driver_internal+0x308/0x478 device_release_driver+0x1c/0x30 bus_remove_device+0x1a8/0x368 device_del+0x2e0/0x7b0 usb_disable_device+0x244/0x540 usb_disconnect+0x220/0x758 hub_event+0x105c/0x35e0 process_one_work+0x760/0x17b0 worker_thread+0x768/0xce8 kthread+0x3bc/0x690 ret_from_fork+0x10/0x20 irq event stamp: 211604 hardirqs last enabled at (211603): [<ffffffc0828cc9ec>] _raw_spin_unlock_irqrestore+0x84/0x98 hardirqs last disabled at (211604): [<ffffffc0828a9a84>] el1_dbg+0x24/0x80 softirqs last enabled at (211296): [<ffffffc080095f10>] handle_softirqs+0x820/0xbc8 softirqs last disabled at (210993): [<ffffffc080010288>] __do_softirq+0x18/0x20 ---[end trace 0000000000000000]--- lan78xx 1-1:1.0 enu1: failed to kill vid 0081/0	N/A	More Details
CVE-2025-38383	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix data race in show_numa_info() The following data-race was found in show_numa_info(): == BUG: KCSAN: data-race in vmalloc_info_show / vmalloc_info_show read to 0xffff88800971fe30 of 4 bytes by task 8289 on cpu 0: show_numa_info mm/vmalloc.c:4936 [inline] vmalloc_info_show+0x5a8/0x7e0 mm/vmalloc.c:5016 seq_read_iter+0x373/0xb40 fs/seq_file.c:230 proc_reg_read_iter+0x11e/0x170 fs/proc/inode.c:299 .... write to 0xffff88800971fe30 of 4 bytes by task 8287 on cpu 1: show_numa_info mm/vmalloc.c:4934 [inline] vmalloc_info_show+0x38f/0x7e0 mm/vmalloc.c:5016 seq_read_iter+0x373/0xb40 fs/seq_file.c:230 proc_reg_read_iter+0x11e/0x170 fs/proc/inode.c:299 .... value changed: 0x0000008f -> 0x00000000 == According to this report,there is a read/write data-race because m->private is accessible to multiple CPUs. To fix this, instead of allocating the heap in proc_vmalloc_init() and passing the heap address to m->private, vmalloc_info_show() should allocate the heap.	N/A	More Details
CVE-2025-38469	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/xen: Fix cleanup logic in emulation of Xen schedop poll hypercalls kvm_xen_schedop_poll does a kmalloc_array() when a VM polls the host for more than one event channel potr (nr_ports > 1). After the kmalloc_array(), the error paths need to go through the "out" label, but the call to kvm_read_guest_virt() does not. [Adjusted commit message. - Paolo]	N/A	More Details
CVE-2025-38382	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix iteration of extrefs during log replay At __inode_add_ref() when processing extrefs, if we jump into the next label we have an undefined value of victim_name.len, since we haven't initialized it before we did the goto. This results in an invalid memory access in the next iteration of the loop since victim_name.len was not initialized to the length of the name of the current extref. Fix this by initializing victim_name.len with the current extref's name length.	N/A	More Details

CVE-2025-38359	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Fix in_atomic() handling in do_secure_storage_access() Kernel user spaces accesses to not exported pages in atomic context incorrectly try to resolve the page fault. With debug options enabled call traces like this can be seen: BUG: sleeping function called from invalid context at kernel/locking/rwsem.c:1523 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 419074, name: qemu-system-s39 preempt_count: 1, expected: 0 RCU nest depth: 0, expected: 0 INFO: lockdep is turned off. Preemption disabled at: [<00000383ea47cfa2>] copy_page_from_iter_atomic+0xa2/0x8a0 CPU: 12 UID: 0 PID: 419074 Comm: qemu-system-s39 Tainted: G W 6.16.0-20250531.rc0.git0.69b3a602feac.63.fc42.s390x+debug #1 PREEMPT Tainted: [W]=WARN Hardware name: IBM 3931 A01 703 (LPAR) Call Trace: [<00000383e990d282>] dump_stack_lvl+0xa2/0xe8 [<00000383e99bf152>] __might_resched+0x292/0x2d0 [<00000383eaa7c374>] down_read+0x34/0x2d0 [<00000383e99432f8>] do_secure_storage_access+0x108/0x360 [<00000383eaa724b0>] __do_pgm_check+0x130/0x220 [<00000383eaa842e4>] pgm_check_handler+0x114/0x160 [<00000383ea47d028>] copy_page_from_iter_atomic+0x128/0x8a0 ([<00000383ea47d016>] copy_page_from_iter_atomic+0x116/0x8a0) [<00000383e9c45eae>] generic_perform_write+0x16e/0x310 [<00000383e9eb87f4>] ext4_buffered_write_iter+0x84/0x160 [<00000383e9da0de4>] vfs_write+0x1c4/0x460 [<00000383e9da123c>] ksys_write+0x7c/0x100 [<00000383eaa7284e>] __do_syscall+0x15e/0x280 [<00000383eaa8417e>] system_call+0x6e/0x90 INFO: lockdep is turned off. It is not allowed to take the mmap_lock while in atomic context. Therefore handle such a secure storage access fault as if the accessed page is not mapped: the uaccess function will return -EFAULT, and the caller has to deal with this. Usually this means that the access is retried in process context, which allows to resolve the page fault (or in this case export the page).	N/A	More Details
CVE-2025-38358	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix race between async reclaim worker and close_ctree() Syzbot reported an assertion failure due to an attempt to add a delayed iput after we have set BTRFS_FS_STATE_NO_DELAYED_IPUT in the fs_info state: WARNING: CPU: 0 PID: 65 at fs/btrfs/inode.c:3420 btrfs_add_delayed_iput+0x2f8/0x370 fs/btrfs/inode.c:3420 Modules linked in: CPU: 0 UID: 0 PID: 65 Comm: kworker/u8:4 Not tainted 6.15.0-next-20250530-syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Workqueue: btrfs-endio-write btrfs_work_helper RIP: 0010:btrfs_add_delayed_iput+0x2f8/0x370 fs/btrfs/inode.c:3420 Code: 4e ad 5d (...) RSP: 0018:ffffc9000213f780 EFLAGS: 00010293 RAX: ffffffff83c635b7 RBX: ffff888058920000 RCX: ffff88801c769e00 RDX: 0000000000000000 RSI: 0000000000000100 RDI: 0000000000000000 RBP: 0000000000000001 R08: ffff888058921b67 R09: 1ffff1100b12436c R10: dffffc0000000000 R11: ffffed100b12436d R12: 0000000000000001 R13: dffffc0000000000 R14: ffff88807d748000 R15: 0000000000000100 FS: 0000000000000000(0000) GS:ffff888125c53000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00002000000bd038 CR3: 000000006a142000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> btrfs_put_ordered_extent+0x19f/0x470 fs/btrfs/ordered-data.c:635 btrfs_finish_one_ordered+0x11d8/0x1b10 fs/btrfs/inode.c:3312 btrfs_work_helper+0x399/0xc20 fs/btrfs/async-thread.c:312 process_one_work kernel/workqueue.c:3238 [inline] process_scheduled_works+0xae1/0x17b0 kernel/workqueue.c:3321 worker_thread+0x8a0/0xda0 kernel/workqueue.c:3402 kthread+0x70e/0x8a0 kernel/kthread.c:464 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> This can happen due to a race with the async reclaim worker like this: 1) The async metadata reclaim worker enters shrink_delalloc(), which calls btrfs_start_delalloc_roots() with an nr_pages argument that has a value less than LONG_MAX, and that in turn enters start_delalloc_inodes(), which sets the local variable 'full_flush' to false because wbc->nr_to_write is less than LONG_MAX; 2) There it finds inode X in a root's delalloc list, grabs a reference for inode X (with igrab()), and triggers writeback for it with filemap_fdatawrite_wbc(), which creates an ordered extent for inode X; 3) The unmount sequence starts from another task, we enter close_ctree() and we flush the workqueue fs_info->endio_write_workers, which waits for the ordered extent for inode X to complete and when dropping the last reference of the ordered extent, with btrfs_put_ordered_extent(), when we call btrfs_add_delayed_iput() we don't add the inode to the list of delayed iputs because it has a refcount of 2, so we decrement it to 1 and return; 4) Shortly after at close_ctree() we call btrfs_run_delayed_iputs() which runs all delayed iputs, and then we set BTRFS_FS_STATE_NO_DELAYED_IPUT in the fs_info state; 5) The async reclaim worker, after calling filemap_fdatawrite_wbc(), now calls btrfs_add_delayed_iput() for inode X and there we trigger an assertion failure since the fs_info state has the flag BTRFS_FS_STATE_NO_DELAYED_IPUT set. Fix this by setting BTRFS_FS_STATE_NO_DELAYED_IPUT only after we wait for the async reclaim workers to finish, after we call cancel_work_sync() for them at close_ctree(), and by running delayed iputs after wait for the reclaim workers to finish and before setting the bit. This race was recently introduced by commit 19e60b2a95f5 ("btrfs: add extra warning if delayed iput is added when it's not allowed"). Without the new validation at btrfs_add_delayed_iput(), ---truncated---	N/A	More Details
CVE-2025-38357	In the Linux kernel, the following vulnerability has been resolved: fuse: fix runtime warning on truncate_folio_batch_exceptionals() The WARN_ON_ONCE is introduced on truncate_folio_batch_exceptionals() to capture whether the filesystem has removed all DAX entries or not. And the fix has been applied on the filesystem xfs and ext4 by the commit 0e2f80afcfa6 ("fs/dax: ensure all pages are idle prior to filesystem unmount"). Apply the missed fix on filesystem fuse to fix the runtime warning: [2.011450] ------------[cut here]------------ [2.011873] WARNING: CPU: 0 PID: 145 at mm/truncate.c:89 truncate_folio_batch_exceptionals+0x272/0x2b0 [2.012468] Modules linked in: [2.012718] CPU: 0 UID: 1000 PID: 145 Comm: weston Not tainted 6.16.0-rc2-WSL2-STABLE #2 PREEMPT(undef) [2.013292] RIP: 0010:truncate_folio_batch_exceptionals+0x272/0x2b0 [2.013704] Code: 48 63 d0 41 29 c5 48 8d 1c d5 00 00 00 00 4e 8d 6c 2a 01 49 c1 e5 03 eb 09 48 83 c3 08 49 39 dd 74 83 41 f6 44 1c 08 01 74 ef <0f> 0b 49 8b 34 1e 48 89 ef e8 10 a2 17 00 eb df 48 8b 7d 00 e8 35 [2.014845] RSP: 0018:ffffa47ec33f3b10 EFLAGS: 00010202 [2.015279] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000 [2.015884] RDX: 0000000000000000 RSI: ffffa47ec33f3ca0 RDI: ffff98aa44f3fa80 [2.016377] RBP: ffff98aa44f3fbf0 R08: ffffa47ec33f3ba8 R09: 0000000000000000 [2.016942] R10: 0000000000000001 R11: 0000000000000000 R12: ffffa47ec33f3ca0 [2.017437] R13: 0000000000000008 R14: ffffa47ec33f3ba8 R15: 0000000000000000 [2.017972] FS: 000079ce006afa40(0000) GS:ffff98aade441000(0000) knlGS:0000000000000000 [2.018510] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [2.018987] CR2: 000079ce03e74000 CR3: 000000010784f006 CR4: 0000000000372eb0 [2.019518] Call Trace: [2.019729] <TASK> [2.019901] truncate_inode_pages_range+0xd8/0x400 [2.020280] ? timerqueue_add+0x66/0xb0 [2.020574] ? get_nohz_timer_target+0x2a/0x140 [2.020904] ? timerqueue_add+0x66/0xb0 [2.021231] ? timerqueue_del+0x2e/0x50 [2.021646] ? __remove_hrtimer+0x39/0x90 [2.022017] ? srso_alias_untrain_ret+0x1/0x10 [2.022497] ? psi_group_change+0x136/0x350 [2.023046] ? _raw_spin_unlock+0xe/0x30 [2.023514] ? finish_task_switch.isra.0+0x8d/0x280 [2.024068] ? __schedule+0x532/0xbd0 [2.024551] fuse_evict_inode+0x29/0x190 [2.025131] evict+0x100/0x270 [2.025641] ? _atomic_dec_and_lock+0x39/0x50 [2.026316] ? __pfx_generic_delete_inode+0x10/0x10 [2.026843] __dentry_kill+0x71/0x180 [2.027335] dput+0xeb/0x1b0 [2.027725] __fput+0x136/0x2b0 [2.028054] __x64_sys_close+0x3d/0x80 [2.028469] do_syscall_64+0x6d/0x1b0 [2.028832] ? clear_bhb_loop+0x30/0x80 [2.029182] ? clear_bhb_loop+0x30/0x80 [2.029533] ? clear_bhb_loop+0x30/0x80 [2.029902] entry_SYSCALL_64_after_hwframe+0x76/0x7e	N/A	More Details

	[2.030423] RIP: 0033:0x79ce03d0d067 [2.030820] Code: b8 ff ff ff ff e9 3e ff ff ff 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75 10 b8 03 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 41 c3 48 83 ec 18 89 7c 24 0c e8 c3 a7 f8 ff [2.032354] RSP: 002b:00007ffef0498948 EFLAGS: 00000246 ORIG_RAX: 0000000000000003 [2.032939] RAX: ffffffffffffffda RBX: 00007ffef0498960 RCX: 000079ce03d0d067 [2.033612] RDX: 0000000000000003 RSI: 0000000000001000 RDI: 000000000000000d [2.034289] RBP: 00007ffef0498a30 R08: 000000000000000d R09: 0000000000000000 [2.034944] R10: 00007ffef0498978 R11: 0000000000000246 R12: 0000000000000001 [2.035610] R13: 00007ffef0498960 R14: 000079ce03e09ce0 R15: 0000000000000003 [2.036301] </TASK> [2.036532] ---[end trace 0000000000000000]---		
CVE-2025-38356	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Explicitly exit CT safe mode on unwind During driver probe we might be briefly using CT safe mode, which is based on a delayed work, but usually we are able to stop this once we have IRQ fully operational. However, if we abort the probe quite early then during unwind we might try to destroy the workqueue while there is still a pending delayed work that attempts to restart itself which triggers a WARN. This was recently observed during unsuccessful VF initialization: [ ] xe 0000:00:02.1: probe with driver xe failed with error -62 [ ] ------------[cut here]------------ [ ] workqueue: cannot queue safe_mode_worker_func [xe] on wq xe-g2h-wq [ ] WARNING: CPU: 9 PID: 0 at kernel/workqueue.c:2257 __queue_work+0x287/0x710 [ ] RIP: 0010:__queue_work+0x287/0x710 [ ] Call Trace: [ ] delayed_work_timer_fn+0x19/0x30 [ ] call_timer_fn+0xa1/0x2a0 Exit the CT safe mode on unwind to avoid that warning. (cherry picked from commit 2ddbb73ec20b98e70a5200cb85deade22ccea2ec)	N/A	More Details
CVE-2025-38355	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Process deferred GGTT node removals on device unwind While we are indirectly draining our dedicated workqueue ggtt->wq that we use to complete asynchronous removal of some GGTT nodes, this happends as part of the managed-drm unwinding (ggtt_fini_early), which could be later then manage-device unwinding, where we could already unmap our MMIO/GMS mapping (mmio_fini). This was recently observed during unsuccessful VF initialization: [ ] xe 0000:00:02.1: probe with driver xe failed with error -62 [ ] xe 0000:00:02.1: DEVRES REL ffff88811e747340 __xe_bo_unpin_map_no_vm (16 bytes) [ ] xe 0000:00:02.1: DEVRES REL ffff88811e747540 __xe_bo_unpin_map_no_vm (16 bytes) [ ] xe 0000:00:02.1: DEVRES REL ffff88811e747240 __xe_bo_unpin_map_no_vm (16 bytes) [ ] xe 0000:00:02.1: DEVRES REL ffff88811e747040 tiles_fini (16 bytes) [ ] xe 0000:00:02.1: DEVRES REL ffff88811e746840 mmio_fini (16 bytes) [ ] xe 0000:00:02.1: DEVRES REL ffff88811e747f40 xe_bo_pinned_fini (16 bytes) [ ] xe 0000:00:02.1: DEVRES REL ffff88811e746b40 devm_drm_dev_init_release (16 bytes) [ ] xe 0000:00:02.1: [drm:drm_managed_release] drmres release begin [ ] xe 0000:00:02.1: [drm:drm_managed_release] REL ffff88810ef81640 __fini_relay (8 bytes) [ ] xe 0000:00:02.1: [drm:drm_managed_release] REL ffff88810ef80d40 guc_ct_fini (8 bytes) [ ] xe 0000:00:02.1: [drm:drm_managed_release] REL ffff88810ef80040 __drmm_mutex_release (8 bytes) [ ] xe 0000:00:02.1: [drm:drm_managed_release] REL ffff88810ef80140 ggtt_fini_early (8 bytes) and this was leading to: [ ] BUG: unable to handle page fault for address: ffffc900058162a0 [ ] #PF: supervisor write access in kernel mode [ ] #PF: error_code(0x0002) - not-present page [ ] Oops: Oops: 0002 [#1] SMP NOPTI [ ] Tainted: [W]=WARN [ ] Workqueue: xe-ggtt-wq ggtt_node_remove_work_func [xe] [ ] RIP: 0010:xe_ggtt_set_pte+0x6d/0x350 [xe] [ ] Call Trace: [ ] <TASK> [ ] xe_ggtt_clear+0xb0/0x270 [xe] [ ] ggtt_node_remove+0xbb/0x120 [xe] [ ] ggtt_node_remove_work_func+0x30/0x50 [xe] [ ] process_one_work+0x22b/0x6f0 [ ] worker_thread+0x1e8/0x3d Add managed-device action that will explicitly drain the workqueue with all pending node removals prior to releasing MMIO/GSM mapping. (cherry picked from commit 89d2835c3680ab1938e22ad81b1c9f8c686bd391)	N/A	More Details
CVE-2025-38354	In the Linux kernel, the following vulnerability has been resolved: drm/msm/gpu: Fix crash when throttling GPU immediately during boot There is a small chance that the GPU is already hot during boot. In that case, the call to of_devfreq_cooling_register() will immediately try to apply devfreq cooling, as seen in the following crash: Unable to handle kernel paging request at virtual address 0000000000014110 pc : a6xx_gpu_busy+0x1c/0x58 [msm] lr : msm_devfreq_get_dev_status+0xbc/0x140 [msm] Call trace: a6xx_gpu_busy+0x1c/0x58 [msm] (P) devfreq_simple_ondemand_func+0x3c/0x150 devfreq_update_target+0x44/0xd8 qos_max_notifier_call+0x30/0x84 blocking_notifier_call_chain+0x6c/0xa0 pm_qos_update_target+0xd0/0x110 freq_qos_apply+0x3c/0x74 apply_constraint+0x88/0x148 __dev_pm_qos_update_request+0x7c/0xcc dev_pm_qos_update_request+0x38/0x5c devfreq_cooling_set_cur_state+0x98/0xf0 __thermal_cdev_update+0x64/0xb4 thermal_cdev_update+0x4c/0x58 step_wise_manage+0x1f0/0x318 __thermal_zone_device_update+0x278/0x424 __thermal_cooling_device_register+0x2bc/0x308 thermal_of_cooling_device_register+0x10/0x1c of_devfreq_cooling_register_power+0x240/0x2bc of_devfreq_cooling_register+0x14/0x20 msm_devfreq_init+0xc4/0x1a0 [msm] msm_gpu_init+0x304/0x574 [msm] adreno_gpu_init+0x1c4/0x2e0 [msm] a6xx_gpu_init+0x5c8/0x9c8 [msm] adreno_bind+0x2a8/0x33c [msm] ... At this point we haven't initialized the GMU at all yet, so we cannot read the GMU registers inside a6xx_gpu_busy(). A similar issue was fixed before in commit 6694482a70e9 ("drm/msm: Avoid unclocked GMU register access in 6xx gpu_busy"): msm_devfreq_init() does call devfreq_suspend_device(), but unlike msm_devfreq_suspend(), it doesn't set the df->suspended flag accordingly. This means the df->suspended flag does not match the actual devfreq state after initialization and msm_devfreq_get_dev_status() will end up accessing GMU registers, causing the crash. Fix this by setting df->suspended correctly during initialization. Patchwork: https://patchwork.freedesktop.org/patch/650772/	N/A	More Details
CVE-2025-38353	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix taking invalid lock on wedge If device wedges on e.g. GuC upload, the submission is not yet enabled and the state is not even initialized. Protect the wedge call so it does nothing in this case. It fixes the following splat: [] xe 0000:bf:00.0: [drm] device wedged, needs recovery [] ------------[cut here]------------ [] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [] WARNING: CPU: 48 PID: 312 at kernel/locking/mutex.c:564 __mutex_lock+0x8a1/0xe60 ... [] RIP: 0010:__mutex_lock+0x8a1/0xe60 [] mutex_lock_nested+0x1b/0x30 [] xe_guc_submit_wedge+0x80/0x2b0 [xe]	N/A	More Details
CVE-2025-7742	An authentication vulnerability exists in the LG Innotek camera model LNV5110R firmware that allows a malicious actor to upload an HTTP POST request to the devices non-volatile storage. This action may result in remote code execution that allows an attacker to run arbitrary commands on the target device at the administrator privilege level.	N/A	More Details
CVE-2025-54379	LF Edge eKuiper is a lightweight IoT data analytics and stream processing engine running on resource-constraint edge devices. In versions before 2.2.1, there is a critical SQL Injection vulnerability in the getLast API functionality of the eKuiper project. This flaw allows unauthenticated remote attackers to execute arbitrary SQL statements on the underlying SQLite database by manipulating the table name input in an API request. Exploitation can lead to data theft, corruption, or deletion, and full database compromise. This is fixed in version 2.2.1.	N/A	More Details
CVE-2025-	Rejected reason: Reason: This candidate was issued in error.	N/A	More Details

54369			
CVE-2025-53940	Quiet is an alternative to team chat apps like Slack, Discord, and Element that does not require trusting a central server or running one's own. In versions 6.1.0-alpha.4 and below, Quiet's API for backend/frontend communication was using an insecure, not constant-time comparison function for token verification. This allowed for a potential timing attack where an attacker would try different token values and observe tiny differences in the response time (wrong characters fail faster) to guess the whole token one character at a time. This is fixed in version 6.0.1.	N/A	More Details
CVE-2025-32429	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions 9.4-rc-1 through 16.10.5 and 17.0.0-rc-1 through 17.2.2, it's possible for anyone to inject SQL using the parameter sort of the getdeleteddocuments.vm. It's injected as is as an ORDER BY value. This is fixed in versions 16.10.6 and 17.3.0-rc-1.	N/A	More Details
CVE-2025-22165	This Medium severity ACE (Arbitrary Code Execution) vulnerability was introduced in version 4.2.8 of Sourcetree for Mac. This ACE (Arbitrary Code Execution) vulnerability, with a CVSS Score of 5.9, allows a locally authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Sourcetree for Mac users upgrade to the latest version. If you are unable to do so, upgrade your instance to one of the specified supported fixed versions. See the release notes https://www.sourcetreeapp.com/download-archives . You can download the latest version of Sourcetree for Mac from the download center https://www.sourcetreeapp.com/download-archives . This vulnerability was found through the Atlassian Bug Bounty Program by Karol Mazurek (AFINE).	N/A	More Details
CVE-2025-7404	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Calibre Web, Autocaliweb allows Blind OS Command Injection.This issue affects Calibre Web: 0.6.24 (Nicolette); Autocaliweb: from 0.7.0 before 0.7.1.	N/A	More Details
CVE-2025-6998	ReDoS in strip_whitespaces() function in cps/string_helper.py in Calibre Web and Autocaliweb allows unauthenticated remote attackers to cause denial of service via specially crafted username parameter that triggers catastrophic backtracking during login. This issue affects Calibre Web: 0.6.24 (Nicolette); Autocaliweb: from 0.7.0 before 0.7.1.	N/A	More Details
CVE-2025-8058	The regcomp function in the GNU C library version from 2.4 to 2.41 is subject to a double free if some previous allocation fails. It can be accomplished either by a malloc failure or by using an interposed malloc that injects random malloc failures. The double free can allow buffer manipulation depending of how the regex is constructed. This issue affects all architectures and ABIs supported by the GNU C library.	N/A	More Details
CVE-2025-40680	Lack of sensitive data encryption in CapillaryScope v2.5.0 of Capillary io, which stores both the proxy credentials and the JWT session token in plain text within different registry keys on the Windows operating system. Any authenticated local user with read access to the registry can extract these sensitive values.	N/A	More Details
CVE-2025-53942	authentik is an open-source Identity Provider that emphasizes flexibility and versatility, with support for a wide set of protocols. In versions 2025.4.4 and earlier, as well as versions 2025.6.0-rc1 through 2025.6.3, deactivated users who registered through OAuth/SAML or linked their accounts to OAuth/SAML providers can still retain partial access to the system despite their accounts being deactivated. They end up in a half-authenticated state where they cannot access the API but crucially they can authorize applications if they know the URL of the application. To workaround this issue, developers can add an expression policy to the user login stage on the respective authentication flow with the expression of return request.context["pending_user"].is_active. This modification ensures that the return statement only activates the user login stage when the user is active. This issue is fixed in versions authentik 2025.4.4 and 2025.6.4.	N/A	More Details
CVE-2025-54365	fastapi-guard is a security library for FastAPI that provides middleware to control IPs, log requests, detect penetration attempts and more. In version 3.0.1, the regular expression patched to mitigate the ReDoS vulnerability by limiting the length of string fails to catch inputs that exceed this limit. This type of patch fails to detect cases in which the string representing the attributes of a <script> tag exceeds 100 characters. As a result, most of the regex patterns present in version 3.0.1 can be bypassed. This is fixed in version 3.0.2.	N/A	More Details
CVE-2025-38360	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add more checks for DSC / HUBP ONO guarantees [WHY] For non-zero DSC instances it's possible that the HUBP domain required to drive it for sequential ONO ASICs isn't met, potentially causing the logic to the tile to enter an undefined state leading to a system hang. [HOW] Add more checks to ensure that the HUBP domain matching the DSC instance is appropriately powered. (cherry picked from commit da63df07112e5a9857a8d2aaa04255c4206754ec)	N/A	More Details
CVE-2025-38361	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check dce_hwseq before dereferencing it [WHAT] hws was checked for null earlier in dce110_blank_stream, indicating hws can be null, and should be checked whenever it is used. (cherry picked from commit 79db43611ff61280b6de58ce1305e0b2ecf675ad)	N/A	More Details
CVE-2025-38362	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null pointer check for get_first_active_display() The function mod_hdcp_hdcp1_enable_encryption() calls the function get_first_active_display(), but does not check its return value. The return value is a null pointer if the display list is empty. This will lead to a null pointer dereference in mod_hdcp_hdcp2_enable_encryption(). Add a null pointer check for get_first_active_display() and return MOD_HDCP_STATUS_DISPLAY_NOT_FOUND if the function return null.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: IB/mlx5: Fix potential deadlock in MR deregistration The issue arises when kzalloc() is invoked while holding umem_mutex or any other lock acquired under umem_mutex. This is problematic because kzalloc() can trigger fs_reclaim_aqcuire(), which may, in turn, invoke mmu_notifier_invalidate_range_start(). This function can lead to mlx5_ib_invalidate_range(), which attempts to acquire umem_mutex again, resulting in a deadlock. The problematic flow: CPU0 | CPU1 --------------------------------------|-- mlx5_ib_dereg_mr() | → revoke_mr() | → mutex_lock(&umem_odp->umem_mutex) | | mlx5_mkey_cache_init() | → mutex_lock(&dev->cache.rb_lock) | → mlx5r_cache_create_ent_locked() | → kzalloc(GFP_KERNEL) | → fs_reclaim() | → mmu_notifier_invalidate_range_start() | → mlx5_ib_invalidate_range() | → mutex_lock(&umem_odp->umem_mutex) → cache_ent_find_and_store() | → mutex_lock(&dev->cache.rb_lock) | Additionally, when kzalloc() is called from within cache_ent_find_and_store(), we encounter the same deadlock due to re-acquisition of umem_mutex. Solve by releasing umem_mutex in dereg_mr() after umr_revoke_mr() and before acquiring rb_lock. This ensures that we don't hold umem_mutex while performing memory allocations that could trigger the reclaim path. This change prevents the deadlock by ensuring proper lock ordering and avoiding holding locks during		

CVE-2025-38373	memory allocation operations that could trigger the reclaim path. The following lockdep warning demonstrates the deadlock: python3/20557 is trying to acquire lock: ffff888387542128 (&umem_odp->umem_mutex){+.+.}-{4:4}, at: mlx5_ib_invalidate_range+0x5b/0x550 [mlx5_ib] but task is already holding lock: ffffffff82f6b840 (mmu_notifier_invalidate_range_start){+.+.}-{0:0}, at: unmap_vmas+0x7b/0x1a0 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #3 (mmu_notifier_invalidate_range_start){+.+.}-{0:0}: fs_reclaim_acquire+0x60/0xd0 mem_cgroup_css_alloc+0x6f/0x9b0 cgroup_init_subsys+0xa4/0x240 cgroup_init+0x1c8/0x510 start_kernel+0x747/0x760 x86_64_start_reservations+0x25/0x30 x86_64_start_kernel+0x73/0x80 common_startup_64+0x129/0x138 -> #2 (fs_reclaim){+.+.}-{0:0}: fs_reclaim_acquire+0x91/0xd0 __kmalloc_cache_noprof+0x4d/0x4c0 mlx5r_cache_create_ent_locked+0x75/0x620 [mlx5_ib] mlx5_mkey_cache_init+0x186/0x360 [mlx5_ib] mlx5_ib_stage_post_ib_reg_umr_init+0x3c/0x60 [mlx5_ib] __mlx5_ib_add+0x4b/0x190 [mlx5_ib] mlx5r_probe+0xd9/0x320 [mlx5_ib] auxiliary_bus_probe+0x42/0x70 really_probe+0xdb/0x360 __driver_probe_device+0x8f/0x130 driver_probe_device+0x1f/0xb0 __driver_attach+0xd4/0x1f0 bus_for_each_dev+0x79/0xd0 bus_add_driver+0xf0/0x200 driver_register+0x6e/0xc0 __auxiliary_driver_register+0x6a/0xc0 do_one_initcall+0x5e/0x390 do_init_module+0x88/0x240 init_module_from_file+0x85/0xc0 idempotent_init_module+0x104/0x300 __x64_sys_finit_module+0x68/0xc0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 -> #1 (&dev->cache.rb_lock){+.+.}-{4:4}: __mutex_lock+0x98/0xf10 __mlx5_ib_dereg_mr+0x6f2/0x890 [mlx5_ib] mlx5_ib_dereg_mr+0x21/0x110 [mlx5_ib] ib_dereg_mr_user+0x85/0x1f0 [ib_core] ---truncated---	N/A	More Details
CVE-2025-38381	In the Linux kernel, the following vulnerability has been resolved: Input: cs40l50-vibra - fix potential NULL dereference in cs40l50_upload_owt() The cs40l50_upload_owt() function allocates memory via kmalloc() without checking for allocation failure, which could lead to a NULL pointer dereference. Return -ENOMEM in case allocation fails.	N/A	More Details
CVE-2025-38380	In the Linux kernel, the following vulnerability has been resolved: i2c/designware: Fix an initialization issue The i2c_dw_xfer_init() function requires msgs and msg_write_idx from the dev context to be initialized. amd_i2c_dw_xfer_quirk() inits msgs and msgs_num, but not msg_write_idx. This could allow an out of bounds access (of msgs). Initialize msg_write_idx before calling i2c_dw_xfer_init().	N/A	More Details
CVE-2025-38379	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix warning when reconnecting channel When reconnecting a channel in smb2_reconnect_server(), a dummy tcon is passed down to smb2_reconnect() with ->query_interface uninitialized, so we can't call queue_delayed_work() on it. Fix the following warning by ensuring that we're queueing the delayed worker from correct tcon. WARNING: CPU: 4 PID: 1126 at kernel/workqueue.c:2498 __queue_delayed_work+0x1d2/0x200 Modules linked in: cifs cifs_arc4 nls_ucs2_utils cifs_md4 [last unloaded: cifs] CPU: 4 UID: 0 PID: 1126 Comm: kworker/4:0 Not tainted 6.16.0-rc3 #5 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-4.fc42 04/01/2014 Workqueue: cifsiod smb2_reconnect_server [cifs] RIP: 0010:__queue_delayed_work+0x1d2/0x200 Code: 41 5e 41 5f e9 7f ee ff ff 90 0f 0b 90 e9 5d ff ff ff bf 02 00 00 00 e8 6c f3 07 00 89 c3 eb bd 90 0f 0b 90 e9 57 f> 0b 90 e9 65 fe ff ff 90 0f 0b 90 e9 72 fe ff ff 90 0f 0b 90 e9 RSP: 0018:ffffc900014afad8 EFLAGS: 00010003 RAX: 0000000000000000 RBX: ffff888124d99988 RCX: ffffffff81399cc1 RDX: dffffc0000000000 RSI: ffff888114326e00 RDI: ffff888124d999f0 RBP: 000000000000ea60 R08: 0000000000000001 R09: ffffed10249b3331 R10: ffff888124d9998f R11: 0000000000000004 R12: 0000000000000040 R13: ffff888114326e00 R14: ffff888124d999d8 R15: ffff888114939020 FS: 0000000000000000(0000) GS:ffff88829f7fe000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffe7a2b4038 CR3: 0000000120a6f000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> queue_delayed_work_on+0xb4/0xc0 smb2_reconnect+0xb22/0xf50 [cifs] smb2_reconnect_server+0x413/0xd40 [cifs] ? __pfx_smb2_reconnect_server+0x10/0x10 [cifs] ? local_clock_noinstr+0xd/0xd0 ? local_clock+0x15/0x30 ? lock_release+0x29b/0x390 process_one_work+0x4c5/0xa10 ? __pfx_process_one_work+0x10/0x10 ? __list_add_valid_or_report+0x37/0x120 worker_thread+0x2f1/0x5a0 ? __kthread_parkme+0xde/0x100 ? __pfx_worker_thread+0x10/0x10 kthread+0x1fe/0x380 ? kthread+0x10f/0x380 ? __pfx_kthread+0x10/0x10 ? local_clock_noinstr+0xd/0xd0 ? ret_from_fork+0x1b/0x1f0 ? local_clock+0x15/0x30 ? lock_release+0x29b/0x390 ? rcu_is_watching+0x20/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x15b/0x1f0 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> irq event stamp: 1116206 hardirqs last enabled at (1116205): [<ffffffff8143af42>] __up_console_sem+0x52/0x60 hardirqs last disabled at (1116206): [<ffffffff81399f0e>] queue_delayed_work_on+0x6e/0xc0 softirqs last enabled at (1116138): [<ffffffffc04562fd>] __smb_send_rqst+0x42d/0x950 [cifs] softirqs last disabled at (1116136): [<ffffffff823d35e1>] release_sock+0x21/0xf0	N/A	More Details
CVE-2025-38378	In the Linux kernel, the following vulnerability has been resolved: HID: appletb-kbd: fix slab use-after-free bug in appletb_kbd_probe In probe appletb_kbd_probe() a "struct appletb_kbd *kbd" is allocated via devm_kzalloc() to store touch bar keyboard related data. Later on if backlight_device_get_by_name() finds a backlight device with name "appletb_backlight" a timer (kbd->inactivity_timer) is setup with appletb_inactivity_timer() and the timer is armed to run after appletb_tb_dim_timeout (60) seconds. A use-after-free is triggered when failure occurs after the timer is armed. This ultimately means probe failure occurs and as a result the "struct appletb_kbd *kbd" which is device managed memory is freed. After 60 seconds the timer will have expired and __run_timers will attempt to access the timer (kbd->inactivity_timer) however the kdb structure has been freed causing a use-after free. [71.636938] == [71.637915] BUG: KASAN: slab-use-after-free in __run_timers+0x7ad/0x890 [71.637915] Write of size 8 at addr ffff8881178c5958 by task swapper/1/0 [71.637915] [71.637915] CPU: 1 UID: 0 PID: 0 Comm: swapper/1 Not tainted 6.16.0-rc2-00318-g739a6c93cc75-dirty #12 PREEMPT(voluntary) [71.637915] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 [71.637915] Call Trace: [71.637915] <IRQ> [71.637915] dump_stack_lvl+0x53/0x70 [71.637915] print_report+0xce/0x670 [71.637915] ? __run_timers+0x7ad/0x890 [71.637915] kasan_report+0xce/0x100 [71.637915] ? __run_timers+0x7ad/0x890 [71.637915] __run_timers+0x7ad/0x890 [71.637915] ? __pfx___run_timers+0x10/0x10 [71.637915] ? update_process_times+0xfc/0x190 [71.637915] ? __pfx_update_process_times+0x10/0x10 [71.637915] ? _raw_spin_lock_irq+0x80/0xe0 [71.637915] ? _raw_spin_lock_irq+0x80/0xe0 [71.637915] ? __pfx__raw_spin_lock_irq+0x10/0x10 [71.637915] run_timer_softirq+0x141/0x240 [71.637915] ? __pfx_run_timer_softirq+0x10/0x10 [71.637915] ? __pfx___hrtimer_run_queues+0x10/0x10 [71.637915] ? kvm_clock_get_cycles+0x18/0x30 [71.637915] ? ktime_get+0x60/0x140 [71.637915] handle_softirqs+0x1b8/0x5c0 [71.637915] ? __pfx_handle_softirqs+0x10/0x10 [71.637915] irq_exit_rcu+0xaf/0xe0 [71.637915] sysvec_apic_timer_interrupt+0x6c/0x80 [71.637915] </IRQ> [71.637915] [71.637915] Allocated by task 39: [71.637915] kasan_save_stack+0x33/0x60 [71.637915] kasan_save_track+0x14/0x30 [71.637915] __kasan_kmalloc+0x8f/0xa0 [71.637915] __kmalloc_node_track_caller_noprof+0x195/0x420 [71.637915] devm_kmalloc+0x74/0x1e0 [71.637915] appletb_kbd_probe+0x37/0x3c0 [71.637915] hid_device_probe+0x2d1/0x680 [71.637915] really_probe+0x1c3/0x690 [71.637915] __driver_probe_device+0x247/0x300 [71.637915] driver_probe_device+0x49/0x210 [...] [71.637915] [71.637915]	N/A	More Details

	Freed by task 39: [71.637915] kasan_save_stack+0x33/0x60 [71.637915] kasan_save_track+0x14/0x30 [71.637915] kasan_save_free_info+0x3b/0x60 [71.637915] __kasan_slab_free+0x37/0x50 [71.637915] kfree+0xcf/0x360 [71.637915] devres_release_group+0x1f8/0x3c0 [71.637915] hid_device_probe+0x315/0x680 [71.637915] really_probe+0x1c3/0x690 [71.637915] __driver_probe_device+0x247/0x300 [71.637915] driver_probe_device+0x49/0x210 [...] The root cause of the issue is that the timer is not disarmed on failure paths leading to it remaining active and accessing freed memory. To fix this call timer_delete_sync() to deactivate the timer. Another small issue is that timer_delete_sync is called unconditionally in appletb_kbd_remove(), fix this by checking for a valid kbd->backlight_dev before calling timer_delete_sync.		
CVE-2025-38377	In the Linux kernel, the following vulnerability has been resolved: rose: fix dangling neighbour pointers in rose_rt_device_down() There are two bugs in rose_rt_device_down() that can cause use-after-free: 1. The loop bound `t->count` is modified within the loop, which can cause the loop to terminate early and miss some entries. 2. When removing an entry from the neighbour array, the subsequent entries are moved up to fill the gap, but the loop index `i` is still incremented, causing the next entry to be skipped. For example, if a node has three neighbours (A, A, B) with count=3 and A is being removed, the second A is not checked. i=0: (A, A, B) -> (A, B) with count=2 ^ checked i=1: (A, B) -> (A, B) with count=2 ^ checked (B, not A!) i=2: (doesn't occur because i < count is false) This leaves the second A in the array with count=2, but the rose_neigh structure has been freed. Code that accesses these entries assumes that the first `count` entries are valid pointers, causing a use-after-free when it accesses the dangling pointer. Fix both issues by iterating over the array in reverse order with a fixed loop bound. This ensures that all entries are examined and that the removal of an entry doesn't affect subsequent iterations.	N/A	More Details
CVE-2025-38376	In the Linux kernel, the following vulnerability has been resolved: usb: chipidea: udc: disconnect/reconnect from host when do suspend/resume Shawn and John reported a hang issue during system suspend as below: - USB gadget is enabled as Ethernet - There is data transfer over USB Ethernet (scp a big file between host and device) - Device is going in/out suspend (echo mem > /sys/power/state) The root cause is the USB device controller is suspended but the USB bus is still active which caused the USB host continues to transfer data with device and the device continues to queue USB requests (in this case, a delayed TCP ACK packet trigger the issue) after controller is suspended, however the USB controller clock is already gated off. Then if udc driver access registers after that point, the system will hang. The correct way to avoid such issue is to disconnect device from host when the USB bus is not at suspend state. Then the host will receive disconnect event and stop data transfer in time. To continue make USB gadget device work after system resume, this will reconnect device automatically. To make usb wakeup work if USB bus is already at suspend state, this will keep connection for it only when USB device controller has enabled wakeup capability.	N/A	More Details
CVE-2025-38375	In the Linux kernel, the following vulnerability has been resolved: virtio-net: ensure the received length does not exceed allocated size In xdp_linearize_page, when reading the following buffers from the ring, we forget to check the received length with the true allocate size. This can lead to an out-of-bound read. This commit adds that missing check.	N/A	More Details
CVE-2025-38374	In the Linux kernel, the following vulnerability has been resolved: optee: ffa: fix sleep in atomic context The OP-TEE driver registers the function notif_callback() for FF-A notifications. However, this function is called in an atomic context leading to errors like this when processing asynchronous notifications: | BUG: sleeping function called from invalid context at kernel/locking/mutex.c:258 | in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 9, name: kworker/0:0 | preempt_count: 1, expected: 0 | RCU nest depth: 0, expected: 0 | CPU: 0 UID: 0 PID: 9 Comm: kworker/0:0 Not tainted 6.14.0-00019-g657536ebe0aa #13 | Hardware name: linux,dummy-virt (DT) | Workqueue: ffa_pcpu_irq_notification notif_pcpu_irq_work_fn | Call trace: | show_stack+0x18/0x24 (C) | dump_stack_lvl+0x78/0x90 | dump_stack+0x18/0x24 | __might_resched+0x114/0x170 | __might_sleep+0x48/0x98 | mutex_lock+0x24/0x80 | optee_get_msg_arg+0x7c/0x21c | simple_call_with_arg+0x50/0xc0 | optee_do_bottom_half+0x14/0x20 | notif_callback+0x3c/0x48 | handle_notif_callbacks+0x9c/0xe0 | notif_get_and_handle+0x40/0x88 | generic_exec_single+0x80/0xc0 | smp_call_function_single+0xfc/0x1a0 | notif_pcpu_irq_work_fn+0x2c/0x38 | process_one_work+0x14c/0x2b4 | worker_thread+0x2e4/0x3e0 | kthread+0x13c/0x210 | ret_from_fork+0x10/0x20 Fix this by adding work queue to process the notification in a non-atomic context.	N/A	More Details
CVE-2025-38372	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix unsafe xarray access in implicit ODP handling __xa_store() and __xa_erase() were used without holding the proper lock, which led to a lockdep warning due to unsafe RCU usage. This patch replaces them with xa_store() and xa_erase(), which perform the necessary locking internally. ============================= WARNING: suspicious RCPU usage 6.14.0-rc7_for_upstream_debug_2025_03_18_15_01 #1 Not tainted ----------------------------- ./include/linux/xarray.h:1211 suspicious rcu_dereference_protected() usage! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 3 locks held by kworker/u136:0/219: at: process_one_work+0xbe4/0x15f0 process_one_work+0x75c/0x15f0 pagefault_mr+0x9a5/0x1390 [mlx5_ib] stack backtrace: CPU: 14 UID: 0 PID: 219 Comm: kworker/u136:0 Not tainted 6.14.0-rc7_for_upstream_debug_2025_03_18_15_01 #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 Workqueue: mlx5_ib_page_fault mlx5_ib_eqe_pf_action [mlx5_ib] Call Trace: dump_stack_lvl+0xa8/0xc0 lockdep_rcu_suspicious+0x1e6/0x260 xas_create+0xb8a/0xee0 xas_store+0x73/0x14c0 __xa_store+0x13c/0x220 ? xa_store_range+0x390/0x390 ? spin_bug+0x1d0/0x1d0 pagefault_mr+0xcb5/0x1390 [mlx5_ib] ? _raw_spin_unlock+0x1f/0x30 mlx5_ib_eqe_pf_action+0x3be/0x2620 [mlx5_ib] ? lockdep_hardirqs_on_prepare+0x400/0x400 ? mlx5_ib_invalidate_range+0xcb0/0xcb0 [mlx5_ib] process_one_work+0x7db/0x15f0 ? pwq_dec_nr_in_flight+0xda0/0xda0 ? assign_work+0x168/0x240 worker_thread+0x57d/0xcd0 ? rescuer_thread+0xc40/0xc40 kthread+0x3b3/0x800 ? kthread_is_per_cpu+0xb0/0xb0 ? lock_downgrade+0x680/0x680 ? do_raw_spin_lock+0x12d/0x270 ? spin_bug+0x1d0/0x1d0 ? finish_task_switch.isra.0+0x284/0x9e0 ? lockdep_hardirqs_on_prepare+0x284/0x400 ? kthread_is_per_cpu+0xb0/0xb0 ret_from_fork+0x2d/0x70 ? kthread_is_per_cpu+0xb0/0xb0 ret_from_fork_asm+0x11/0x20	N/A	More Details
CVE-2025-38363	In the Linux kernel, the following vulnerability has been resolved: drm/tegra: Fix a possible null pointer dereference In tegra_crtc_reset(), new memory is allocated with kzalloc(), but no check is performed. Before calling __drm_atomic_helper_crtc_reset, state should be checked to prevent possible null pointer dereference.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Disable interrupts before resetting the GPU Currently, an interrupt can be triggered during a GPU reset, which can lead to GPU hangs and NULL pointer dereference in an interrupt context as shown in the following trace: [314.035040] Unable to handle kernel NULL pointer dereference at virtual address 00000000000000c0 [314.043822] Mem abort info: [314.046606] ESR = 0x0000000096000005 [314.050347] EC = 0x25: DABT (current EL), IL = 32 bits [314.055651] SET = 0, FnV = 0 [314.058695] EA = 0, S1PTW = 0 [314.061826] FSC = 0x05: level 1 translation fault [314.066694] Data abort info: [314.069564] ISV = 0, ISS = 0x00000005, ISS2 = 0x00000000 [314.075039] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [314.080080] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [		

CVE-2025-38371	314.085382] user pgtable: 4k pages, 39-bit VAs, pgdp=0000000102728000 [314.091814] [00000000000000c0] pgd=0000000000000000, p4d=0000000000000000, pud=0000000000000000 [314.100511] Internal error: Oops: 0000000096000005 [#1] PREEMPT SMP [314.106770] Modules linked in: v3d i2c_brcmstb vc4 snd_soc_hdmi_codec gpu_sched drm_shmem_helper drm_display_helper cec drm_dma_helper drm_kms_helper drm drm_panel_orientation_quirks snd_soc_core snd_compress snd_pcm_dmaengine snd_pcm snd_timer snd backlight [314.129654] CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Not tainted 6.12.25+rpt-rpi-v8 #1 Debian 1:6.12.25-1+rpt1 [314.139388] Hardware name: Raspberry Pi 4 Model B Rev 1.4 (DT) [314.145211] pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [314.152165] pc : v3d_irq+0xec/0x2e0 [v3d] [314.156187] lr : v3d_irq+0xe0/0x2e0 [v3d] [314.160198] sp : ffffffc080003ea0 [314.163502] x29: ffffffc080003ea0 x28: ffffffec1f184980 x27: 021202b000000000 [314.170633] x26: ffffffec1f17f630 x25: ffffff8101372000 x24: ffffffec1f17d9f0 [314.177764] x23: 000000000000002a x22: 000000000000002a x21: ffffff8103252000 [314.184895] x20: 0000000000000001 x19: 00000000deadbeef x18: 0000000000000000 [314.192026] x17: ffffff94e51d2000 x16: ffffffec1dac3cb0 x15: c306000000000000 [314.199156] x14: 0000000000000000 x13: b2fc982e03cc5168 x12: 0000000000000001 [314.206286] x11: ffffff8103f8bcc0 x10: ffffffec1f196868 x9 : ffffffec1dac3874 [314.213416] x8 : 0000000000000000 x7 : 0000000000042a3a x6 : ffffff810017a180 [314.220547] x5 : ffffffec1ebad400 x4 : ffffffec1ebad320 x3 : 00000000000bebeb [314.227677] x2 : 0000000000000000 x1 : 0000000000000000 x0 : 0000000000000000 [314.234807] Call trace: [314.237243] v3d_irq+0xec/0x2e0 [v3d] [314.240906] __handle_irq_event_percpu+0x58/0x218 [314.245609] handle_irq_event+0x54/0xb8 [314.249439] handle_fasteoi_irq+0xac/0x240 [314.253527] handle_irq_desc+0x48/0x68 [314.257269] generic_handle_domain_irq+0x24/0x38 [314.261879] gic_handle_irq+0x48/0xd8 [314.265533] call_on_irq_stack+0x24/0x58 [314.269448] do_interrupt_handler+0x88/0x98 [314.273624] el1_interrupt+0x34/0x68 [314.277193] el1h_64_irq_handler+0x18/0x28 [314.281281] el1h_64_irq+0x64/0x68 [314.284673] default_idle_call+0x3c/0x168 [314.288675] do_idle+0x1fc/0x230 [314.291895] cpu_startup_entry+0x3c/0x50 [314.295810] rest_init+0xe4/0xf0 [314.299030] start_kernel+0x5e8/0x790 [314.302684] __primary_switched+0x80/0x90 [314.306691] Code: 940029eb 360ffc13 f9442ea0 52800001 (f9406017) [314.312775] ---[end trace 0000000000000000]--- [314.317384] Kernel panic - not syncing: Oops: Fatal exception in interrupt [314.324249] SMP: stopping secondary CPUs [314.328167] Kernel Offset: 0x2b9da00000 from 0xffffffc080000000 [314.334076] PHYS_OFFSET: 0x0 [314.336946] CPU features: 0x08,00002013,c0200000,0200421b [314.342337] Memory Limit: none [314.345382] ---[end Kernel panic - not syncing: Oops: Fatal exception in interrupt]--- Before resetting the G ---truncated---	N/A	More Details
CVE-2025-38370	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix failure to rebuild free space tree using multiple transactions If we are rebuilding a free space tree, while modifying the free space tree we may need to allocate a new metadata block group. If we end up using multiple transactions for the rebuild, when we call btrfs_end_transaction() we enter btrfs_create_pending_block_groups() which calls add_block_group_free_space() to add items to the free space tree for the block group. Then later during the free space tree rebuild, at btrfs_rebuild_free_space_tree(), we may find such new block groups and call populate_free_space_tree() for them, which fails with -EEXIST because there are already items in the free space tree. Then we abort the transaction with -EEXIST at btrfs_rebuild_free_space_tree(). Notice that we say "may find" the new block groups because a new block group may be inserted in the block groups rbtree, which is being iterated by the rebuild process, before or after the current node where the rebuild process is currently at. Syzbot recently reported such case which produces a trace like the following: ------------[cut here]------------ BTRFS: Transaction aborted (error -17) WARNING: CPU: 1 PID: 7626 at fs/btrfs/free-space-tree.c:1341 btrfs_rebuild_free_space_tree+0x470/0x54c fs/btrfs/free-space-tree.c:1341 Modules linked in: CPU: 1 UID: 0 PID: 7626 Comm: syz.2.25 Not tainted 6.15.0-rc7-syzkaller-00085-gd7fa1af5b33e-dirty #0 PREEMPT Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : btrfs_rebuild_free_space_tree+0x470/0x54c fs/btrfs/free-space-tree.c:1341 lr : btrfs_rebuild_free_space_tree+0x470/0x54c fs/btrfs/free-space-tree.c:1341 sp : ffff80009c4f7740 x29: ffff80009c4f77b0 x28: ffff0000d4c3f400 x27: 0000000000000000 x26: dfff800000000000 x25: ffff70001389eee8 x24: 0000000000000003 x23: 1fffe000182b6e7b x22: 0000000000000000 x21: ffff0000c15b73d8 x20: 00000000ffffffef x19: ffff0000c15b7378 x18: 1fffe0003386f276 x17: ffff80008f31e000 x16: ffff80008adbe98c x15: 0000000000000001 x14: 1fffe0001b281550 x13: 0000000000000000 x12: 0000000000000000 x11: ffff60001b281551 x10: 0000000000000003 x9 : 1c8922000a902c00 x8 : 1c8922000a902c00 x7 : ffff800080485878 x6 : 0000000000000000 x5 : 0000000000000001 x4 : 0000000000000001 x3 : ffff80008047843c x2 : 0000000000000001 x1 : ffff80008b3ebc40 x0 : 0000000000000001 Call trace: btrfs_rebuild_free_space_tree+0x470/0x54c fs/btrfs/free-space-tree.c:1341 (P) btrfs_start_pre_rw_mount+0xa78/0xe10 fs/btrfs/disk-io.c:3074 btrfs_remount_rw fs/btrfs/super.c:1319 [inline] btrfs_reconfigure+0x828/0x2418 fs/btrfs/super.c:1543 reconfigure_super+0x1d4/0x6f0 fs/super.c:1083 do_remount fs/namespace.c:3365 [inline] path_mount+0xb34/0xde0 fs/namespace.c:4200 do_mount fs/namespace.c:4221 [inline] __do_sys_mount fs/namespace.c:4432 [inline] __se_sys_mount fs/namespace.c:4409 [inline] __arm64_sys_mount+0x3e8/0x468 fs/namespace.c:4409 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x98/0x2b8 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x130/0x23c arch/arm64/kernel/syscall.c:132 do_el0_svc+0x48/0x58 arch/arm64/kernel/syscall.c:151 el0_svc+0x58/0x17c arch/arm64/kernel/entry-common.c:767 el0t_64_sync_handler+0x78/0x108 arch/arm64/kernel/entry-common.c:786 el0t_64_sync+0x198/0x19c arch/arm64/kernel/entry.S:600 irq event stamp: 330 hardirqs last enabled at (329): [<ffff80008048590c>] raw_spin_rq_unlock_irq kernel/sched/sched.h:1525 [inline] hardirqs last enabled at (329): [<ffff80008048590c>] finish_lock_switch+0xb0/0x1c0 kernel/sched/core.c:5130 hardirqs last disabled at (330): [<ffff80008adb9e60>] el1_dbg+0x24/0x80 arch/arm64/kernel/entry-common.c:511 softirqs last enabled at (10): [<ffff8000801fbf10>] local_bh_enable+0 ---truncated---	N/A	More Details
CVE-2025-38369	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Check availability of workqueue allocated by idxd wq driver before using Running IDXD workloads in a container with the /dev directory mounted can trigger a call trace or even a kernel panic when the parent process of the container is terminated. This issue occurs because, under certain configurations, Docker does not properly propagate the mount replica back to the original mount point. In this case, when the user driver detaches, the WQ is destroyed but it still calls destroy_workqueue() attempting to completes all pending work. It's necessary to check wq->wq and skip the drain if it no longer exists.	N/A	More Details
CVE-2025-38368	In the Linux kernel, the following vulnerability has been resolved: misc: tps6594-pfsm: Add NULL pointer check in tps6594_pfsm_probe() The returned value, pfsm->miscdev.name, from devm_kasprintf() could be NULL. A pointer check is added to prevent potential NULL pointer dereference. This is similar to the fix in commit 3027e7b15b02 ("ice: Fix some null pointer dereference issues in ice_ptp.c"). This issue is found by our static analysis tool.	N/A	More Details
CVE-2025-38367	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Avoid overflow with array index The variable index is modified and reused as array index when modify register EIOINTC_ENABLE. There will be array index overflow problem.	N/A	More Details

CVE-2025-38366	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Check validity of "num_cpu" from user space The maximum supported cpu number is EIOINTC_ROUTE_MAX_VCPUS about irqchip EIOINTC, here add validation about cpu number to avoid array pointer overflow.	N/A	More Details
CVE-2025-38365	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix a race between renames and directory logging We have a race between a rename and directory inode logging that if it happens and we crash/power fail before the rename completes, the next time the filesystem is mounted, the log replay code will end up deleting the file that was being renamed. This is best explained following a step by step analysis of an interleaving of steps that lead into this situation. Consider the initial conditions: 1) We are at transaction N; 2) We have directories A and B created in a past transaction (< N); 3) We have inode X corresponding to a file that has 2 hardlinks, one in directory A and the other in directory B, so we'll name them as "A/foo_link1" and "B/foo_link2". Both hard links were persisted in a past transaction (< N); 4) We have inode Y corresponding to a file that as a single hard link and is located in directory A, we'll name it as "A/bar". This file was also persisted in a past transaction (< N). The steps leading to a file loss are the following and for all of them we are under transaction N: 1) Link "A/foo_link1" is removed, so inode's X last_unlink_trans field is updated to N, through btrfs_unlink() -> btrfs_record_unlink_dir(); 2) Task A starts a rename for inode Y, with the goal of renaming from "A/bar" to "A/baz", so we enter btrfs_rename(); 3) Task A inserts the new BTRFS_INODE_REF_KEY for inode Y by calling btrfs_insert_inode_ref(); 4) Because the rename happens in the same directory, we don't set the last_unlink_trans field of directoty A's inode to the current transaction id, that is, we don't cal btrfs_record_unlink_dir(); 5) Task A then removes the entries from directory A (BTRFS_DIR_ITEM_KEY and BTRFS_DIR_INDEX_KEY items) when calling __btrfs_unlink_inode() (actually the dir index item is added as a delayed item, but the effect is the same); 6) Now before task A adds the new entry "A/baz" to directory A by calling btrfs_add_link(), another task, task B is logging inode X; 7) Task B starts a fsync of inode X and after logging inode X, at btrfs_log_inode_parent() it calls btrfs_log_all_parents(), since inode X has a last_unlink_trans value of N, set at in step 1; 8) At btrfs_log_all_parents() we search for all parent directories of inode X using the commit root, so we find directories A and B and log them. Bu when logging direct A, we don't have a dir index item for inode Y anymore, neither the old name "A/bar" nor for the new name "A/baz" since the rename has deleted the old name but has not yet inserted the new name - task A hasn't called yet btrfs_add_link() to do that. Note that logging directory A doesn't fallback to a transaction commit because its last_unlink_trans has a lower value than the current transaction's id (see step 4); 9) Task B finishes logging directories A and B and gets back to btrfs_sync_file() where it calls btrfs_sync_log() to persist the log tree; 10) Task B successfully persisted the log tree, btrfs_sync_log() completed with success, and a power failure happened. We have a log tree without any directory entry for inode Y, so the log replay code deletes the entry for inode Y, name "A/bar", from the subvolume tree since it doesn't exist in the log tree and the log tree is authorative for its index (we logged a BTRFS_DIR_LOG_INDEX_KEY item that covers the index range for the dentry that corresponds to "A/bar"). Since there's no other hard link for inode Y and the log replay code deletes the name "A/bar", the file is lost. The issue wouldn't happen if task B synced the log only after task A called btrfs_log_new_name(), which would update the log with the new name for inode Y ("A/bar"). Fix this by pinning the log root during renames before removing the old directory entry, and unpinning af ---truncated---	N/A	More Details
CVE-2025-38364	In the Linux kernel, the following vulnerability has been resolved: maple_tree: fix MA_STATE_PREALLOC flag in mas_preallocate() Temporarily clear the preallocation flag when explicitly requesting allocations. Pre-existing allocations are already counted against the request through mas_node_count_gfp(), but the allocations will not happen if the MA_STATE_PREALLOC flag is set. This flag is meant to avoid re-allocating in bulk allocation mode, and to detect issues with preallocation calculations. The MA_STATE_PREALLOC flag should also always be set on zero allocations so that detection of underflow allocations will print a WARN_ON() during consumption. User visible effect of this flaw is a WARN_ON() followed by a null pointer dereference when subsequent requests for larger number of nodes is ignored, such as the vma merge retry in mmap_region() caused by drivers altering the vma flags (which happens in v6.6, at least)	N/A	More Details
CVE-2025-38427	In the Linux kernel, the following vulnerability has been resolved: video: screen_info: Relocate framebuffers behind PCI bridges Apply PCI host-bridge window offsets to screen_info framebuffers. Fixes invalid access to I/O memory. Resources behind a PCI host bridge can be relocated by a certain offset in the kernel's CPU address range used for I/O. The framebuffer memory range stored in screen_info refers to the CPU addresses as seen during boot (where the offset is 0). During boot up, firmware may assign a different memory offset to the PCI host bridge and thereby relocating the framebuffer address of the PCI graphics device as seen by the kernel. The information in screen_info must be updated as well. The helper pcibios_bus_to_resource() performs the relocation of the screen_info's framebuffer resource (given in PCI bus addresses). The result matches the I/O-memory resource of the PCI graphics device (given in CPU addresses). As before, we store away the information necessary to later update the information in screen_info itself. Commit 78aa89d1dfba ("firmware/sysfb: Update screen_info for relocated EFI framebuffers") added the code for updating screen_info. It is based on similar functionality that pre-existed in efifb. Efifb uses a pointer to the PCI resource, while the newer code does a memcpy of the region. Hence efifb sees any updates to the PCI resource and avoids the issue. v3: - Only use struct pci_bus_region for PCI bus addresses (Bjorn) - Clarify address semantics in commit messages and comments (Bjorn) v2: - Fixed tags (Takashi, Ivan) - Updated information on efifb	N/A	More Details
CVE-2025-38428	In the Linux kernel, the following vulnerability has been resolved: Input: ims-pcu - check record size in ims_pcu_flash_firmware() The "len" variable comes from the firmware and we generally do trust firmware, but it's always better to double check. If the "len" is too large it could result in memory corruption when we do "memcpy(fragment->data, rec->data, len);"	N/A	More Details
CVE-2025-38429	In the Linux kernel, the following vulnerability has been resolved: bus: mhi: ep: Update read pointer only after buffer is written Inside mhi_ep_ring_add_element, the read pointer (rd_offset) is updated before the buffer is written, potentially causing race conditions where the host sees an updated read pointer before the buffer is actually written. Updating rd_offset prematurely can lead to the host accessing an uninitialized or incomplete element, resulting in data corruption. Invoke the buffer write before updating rd_offset to ensure the element is fully written before signaling its availability.	N/A	More Details
CVE-2025-38430	In the Linux kernel, the following vulnerability has been resolved: nfsd: nfsd4_spo_must_allow() must check this is a v4 compound request If the request being processed is not a v4 compound request, then examining the cstate can have undefined results. This patch adds a check that the rpc procedure being executed (rq_procinfo) is the NFSPROC4_COMPOUND procedure.	N/A	More Details
CVE-2016-15045	A local privilege escalation vulnerability exists in lastore-daemon, the system package manager daemon used in Deepin Linux (developed by Wuhan Deepin Technology Co., Ltd.). In versions 0.9.53-1 (Deepin 15.5) and 0.9.66-1 (Deepin 15.7), the D-Bus configuration permits any user in the sudo group to invoke the InstallPackage method without password authentication. By default, the first user created on Deepin is in the sudo group. An attacker with shell access can craft a .deb package containing a malicious post-install script and use dbus-send to install it via lastore-daemon, resulting in arbitrary code execution as root.	N/A	More Details
	The Marathon UI in DC/OS < 1.9.0 allows unauthenticated users to deploy arbitrary Docker containers. Due to improper		

CVE-2017-20198	restriction of volume mount configurations, attackers can deploy a container that mounts the host's root filesystem (/) with read/write privileges. When using a malicious Docker image, the attacker can write to /etc/cron.d/ on the host, achieving arbitrary code execution with root privileges. This impacts any system where the Docker daemon honors Marathon container configurations without policy enforcement.	N/A	More Details
CVE-2018-25113	An unauthenticated path traversal vulnerability exists in Dicoogle PACS Web Server version 2.5.0 and possibly earlier. The vulnerability allows remote attackers to read arbitrary files on the underlying system by sending a crafted request to the /exportFile endpoint using the UID parameter. Successful exploitation can reveal sensitive files accessible by the web server user.	N/A	More Details
CVE-2018-25114	A remote code execution vulnerability exists within osCommerce Online Merchant version 2.3.4.1 due to insecure default configuration and missing authentication in the installer workflow. By default, the /install/ directory remains accessible after installation. An unauthenticated attacker can invoke install_4.php, submit crafted POST data, and inject arbitrary PHP code into the configure.php file. When the application later includes this file, the injected payload is executed, resulting in full server-side compromise.	N/A	More Details
CVE-2022-4978	Remote Control Server, maintained by Steppschuh, 3.1.1.12 allows unauthenticated remote code execution when authentication is disabled, which is the default configuration. The server exposes a custom UDP-based control protocol that accepts remote keyboard input events without verification. An attacker on the same network can issue a sequence of keystroke commands to launch a system shell and execute arbitrary commands, resulting in full system compromise.	N/A	More Details
CVE-2025-43484	A potential reflected cross-site scripting vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The website does not validate or sanitize the user input before rendering it in the response. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-3873	The following APIs for the Silcon Labs SiWx91x prior to vesion 3.4.0 failed to check the size of the output buffer of the caller which could lead to data corruption on the host (Cortex-M4) application. sl_si91x_aes sl_si91x_gcm sl_si91x_ccm sl_si91x_sha	N/A	More Details
CVE-2025-3508	Certain HP DesignJet products may be vulnerable to information disclosure though printer's web interface allowing unauthenticated users to view sensitive print job information.	N/A	More Details
CVE-2025-38467	In the Linux kernel, the following vulnerability has been resolved: drm/exynos: exynos7_drm_decon: add vblank check in IRQ handling If there's support for another console device (such as a TTY serial), the kernel occasionally panics during boot. The panic message and a relevant snippet of the call stack is as follows: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Call trace: drm_crtc_handle_vblank+0x10/0x30 (P) decon_irq_handler+0x88/0xb4 [...] Otherwise, the panics don't happen. This indicates that it's some sort of race condition. Add a check to validate if the drm device can handle vblanks before calling drm_crtc_handle_vblank() to avoid this.	N/A	More Details
CVE-2025-38466	In the Linux kernel, the following vulnerability has been resolved: perf: Revert to requiring CAP_SYS_ADMIN for uprobes Jann reports that uprobes can be used destructively when used in the middle of an instruction. The kernel only verifies there is a valid instruction at the requested offset, but due to variable instruction length cannot determine if this is an instruction as seen by the intended execution stream. Additionally, Mark Rutland notes that on architectures that mix data in the text segment (like arm64), a similar things can be done if the data word is 'mistaken' for an instruction. As such, require CAP_SYS_ADMIN for uprobes.	N/A	More Details
CVE-2025-38465	In the Linux kernel, the following vulnerability has been resolved: netlink: Fix wraparounds of sk->sk_rmem_alloc. Netlink has this pattern in some places if (atomic_read(&sk->sk_rmem_alloc) > sk->sk_rcvbuf) atomic_add(skb->truesize, &sk->sk_rmem_alloc); , which has the same problem fixed by commit 5a465a0da13e ("udp: Fix multiple wraparounds of sk->sk_rmem_alloc."). For example, if we set INT_MAX to SO_RCVBUFFORCE, the condition is always false as the two operands are of int. Then, a single socket can eat as many skb as possible until OOM happens, and we can see multiple wraparounds of sk->sk_rmem_alloc. Let's fix it by using atomic_add_return() and comparing the two variables as unsigned int. Before: [root@fedora ~]# ss -f netlink Recv-Q Send-Q Local Address:Port Peer Address:Port -1668710080 0 rtnl:nl_wraparound/293 * After: [root@fedora ~]# ss -f netlink Recv-Q Send-Q Local Address:Port Peer Address:Port 2147483072 0 rtnl:nl_wraparound/290 * ^ `--- INT_MAX - 576	N/A	More Details
CVE-2025-38464	In the Linux kernel, the following vulnerability has been resolved: tipc: Fix use-after-free in tipc_conn_close(). syzbot reported a null-ptr-deref in tipc_conn_close() during netns dismantle. [0] tipc_topsrv_stop() iterates tipc_net(net)->topsrv->conn_idr and calls tipc_conn_close() for each tipc_conn. The problem is that tipc_conn_close() is called after releasing the IDR lock. At the same time, there might be tipc_conn_recv_work() running and it could call tipc_conn_close() for the same tipc_conn and release its last ->kref. Once we release the IDR lock in tipc_topsrv_stop(), there is no guarantee that the tipc_conn is alive. Let's hold the ref before releasing the lock and put the ref after tipc_conn_close() in tipc_topsrv_stop(). [0]: BUG: KASAN: use-after-free in tipc_conn_close+0x122/0x140 net/tipc/topsrv.c:165 Read of size 8 at addr ffff888099305a08 by task kworker/u4:3/435 CPU: 0 PID: 435 Comm: kworker/u4:3 Not tainted 4.19.204-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Workqueue: netns cleanup_net Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x1fc/0x2ef lib/dump_stack.c:118 print_address_description.cold+0x54/0x219 mm/kasan/report.c:256 kasan_report_error.cold+0x8a/0x1b9 mm/kasan/report.c:354 kasan_report mm/kasan/report.c:412 [inline] __asan_report_load8_noabort+0x88/0x90 mm/kasan/report.c:433 tipc_conn_close+0x122/0x140 net/tipc/topsrv.c:165 tipc_topsrv_stop net/tipc/topsrv.c:701 [inline] tipc_topsrv_exit_net+0x27b/0x5c0 net/tipc/topsrv.c:722 ops_exit_list+0xa5/0x150 net/core/net_namespace.c:153 cleanup_net+0x3b4/0x8b0 net/core/net_namespace.c:553 process_one_work+0x864/0x1570 kernel/workqueue.c:2153 worker_thread+0x64c/0x1130 kernel/workqueue.c:2296 kthread+0x33f/0x460 kernel/kthread.c:259 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:415 Allocated by task 23: kmem_cache_alloc_trace+0x12f/0x380 mm/slab.c:3625 kmalloc include/linux/slab.h:515 [inline] kzalloc include/linux/slab.h:709 [inline] tipc_conn_alloc+0x43/0x4f0 net/tipc/topsrv.c:192 tipc_topsrv_accept+0x1b5/0x280 net/tipc/topsrv.c:470 process_one_work+0x864/0x1570 kernel/workqueue.c:2153 worker_thread+0x64c/0x1130 kernel/workqueue.c:2296 kthread+0x33f/0x460 kernel/kthread.c:259 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:415 Freed by task 23: __cache_free mm/slab.c:3503 [inline] kfree+0xcc/0x210 mm/slab.c:3822 tipc_conn_kref_release net/tipc/topsrv.c:150 [inline] kref_put include/linux/kref.h:70 [inline] conn_put+0x2cd/0x3a0 net/tipc/topsrv.c:155 process_one_work+0x864/0x1570 kernel/workqueue.c:2153 worker_thread+0x64c/0x1130 kernel/workqueue.c:2296 kthread+0x33f/0x460 kernel/kthread.c:259 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:415 The buggy address belongs to the object at ffff888099305a00 which belongs to the cache	N/A	More Details

	kmalloc-512 of size 512 The buggy address is located 8 bytes inside of 512-byte region [ffff888099305a00, ffff888099305c00) The buggy address belongs to the page: page:ffffea000264c140 count:1 mapcount:0 mapping:ffff88813bff0940 index:0x0 flags: 0xfff00000000100(slab) raw: 00fff00000000100 ffffea00028b6b88 ffffea0002cd2b08 ffff88813bff0940 raw: 0000000000000000 ffff888099305000 0000000100000006 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff888099305900: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff888099305980: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc >ffff888099305a00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff888099305a80: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff888099305b00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb		
CVE-2025-38463	In the Linux kernel, the following vulnerability has been resolved: tcp: Correct signedness in skb remaining space calculation Syzkaller reported a bug [1] where sk->sk_forward_alloc can overflow. When we send data, if an skb exists at the tail of the write queue, the kernel will attempt to append the new data to that skb. However, the code that checks for available space in the skb is flawed: ''' copy = size_goal - skb->len ''' The types of the variables involved are: ''' copy: ssize_t (s64 on 64-bit systems) size_goal: int skb->len: unsigned int ''' Due to C's type promotion rules, the signed size_goal is converted to an unsigned int to match skb->len before the subtraction. The result is an unsigned int. When this unsigned int result is then assigned to the s64 copy variable, it is zero-extended, preserving its non-negative value. Consequently, copy is always >= 0. Assume we are sending 2GB of data and size_goal has been adjusted to a value smaller than skb->len. The subtraction will result in copy holding a very large positive integer. In the subsequent logic, this large value is used to update sk->sk_forward_alloc, which can easily cause it to overflow. The syzkaller reproducer uses TCP_REPAIR to reliably create this condition. However, this can also occur in real-world scenarios. The tcp_bound_to_half_wnd() function can also reduce size_goal to a small value. This would cause the subsequent tcp_wmem_schedule() to set sk->sk_forward_alloc to a value close to INT_MAX. Further memory allocation requests would then cause sk_forward_alloc to wrap around and become negative. [1]: https://syzkaller.appspot.com/bug?extid=de6565462ab540f50e47	N/A	More Details
CVE-2025-38462	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix transport_{g2h,h2g} TOCTOU vsock_find_cid() and vsock_dev_do_ioctl() may race with module unload. transport_{g2h,h2g} may become NULL after the NULL check. Introduce vsock_transport_local_cid() to protect from a potential null-ptr-deref. KASAN: null-ptr-deref in range [0x0000000000000118-0x000000000000011f] RIP: 0010:vsock_find_cid+0x47/0x90 Call Trace: __vsock_bind+0x4b2/0x720 vsock_bind+0x90/0xe0 __sys_bind+0x14d/0x1e0 __x64_sys_bind+0x6e/0xc0 do_syscall_64+0x92/0x1c0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 KASAN: null-ptr-deref in range [0x0000000000000118-0x000000000000011f] RIP: 0010:vsock_dev_do_ioctl.isra.0+0x58/0xf0 Call Trace: __x64_sys_ioctl+0x12d/0x190 do_syscall_64+0x92/0x1c0 entry_SYSCALL_64_after_hwframe+0x4b/0x53	N/A	More Details
CVE-2025-38461	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix transport_* TOCTOU Transport assignment may race with module unload. Protect new_transport from becoming a stale pointer. This also takes care of an insecure call in vsock_use_local_transport(); add a lockdep assert. BUG: unable to handle page fault for address: fffffbfff8056000 Oops: Oops: 0000 [#1] SMP KASAN RIP: 0010:vsock_assign_transport+0x366/0x600 Call Trace: vsock_connect+0x59c/0xc40 __sys_connect+0xe8/0x100 __x64_sys_connect+0x6e/0xc0 do_syscall_64+0x92/0x1c0 entry_SYSCALL_64_after_hwframe+0x4b/0x53	N/A	More Details
CVE-2025-38460	In the Linux kernel, the following vulnerability has been resolved: atm: clip: Fix potential null-ptr-deref in to_atmarpd(). atmarpd is protected by RTNL since commit f3a0592b37b8 ("[ATM]: clip causes unregister hang"). However, it is not enough because to_atmarpd() is called without RTNL, especially clip_neigh_solicit() / neigh_ops->solicit() is unsleepable. Also, there is no RTNL dependency around atmarpd. Let's use a private mutex and RCU to protect access to atmarpd in to_atmarpd().	N/A	More Details
CVE-2025-38459	In the Linux kernel, the following vulnerability has been resolved: atm: clip: Fix infinite recursive call of clip_push(). syzbot reported the splat below. [0] This happens if we call ioctl(ATMARP_MKIP) more than once. During the first call, clip_mkip() sets clip_push() to vcc->push(), and the second call copies it to clip_vcc->old_push(). Later, when the socket is close()d, vcc_destroy_socket() passes NULL skb to clip_push(), which calls clip_vcc->old_push(), triggering the infinite recursion. Let's prevent the second ioctl(ATMARP_MKIP) by checking vcc->user_back, which is allocated by the first call as clip_vcc. Note also that we use lock_sock() to prevent racy calls. [0]: BUG: TASK stack guard page was hit at ffffc9000d66fff8 (stack is ffffc9000d670000..ffffc9000d678000) Oops: stack guard page: 0000 [#1] SMP KASAN NOPTI CPU: 0 UID: 0 PID: 5322 Comm: syz.0.0 Not tainted 6.16.0-rc4-syzkaller #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:clip_push+0x5/0x720 net/atm/clip.c:191 Code: e0 8f aa 8c e8 1c ad 5b fa eb ae 66 2e 0f 1f 84 00 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 55 <41> 57 41 56 41 55 41 54 53 48 83 ec 20 48 89 f3 49 89 fd 48 bd 00 RSP: 0018:ffffc9000d670000 EFLAGS: 00010246 RAX: 1ffff1100235a4a5 RBX: ffff888011ad2508 RCX: ffff8880003c0000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff888037f01000 RBP: dffffc0000000000 R08: ffffffff8fa104f7 R09: 1ffffffff1f4209e R10: dffffc0000000000 R11: ffffffff8a99b300 R12: ffffffff8a99b300 R13: ffff888037f01000 R14: ffff888011ad2500 R15: ffff888037f01578 FS: 000055557ab6d500(0000) GS:ffff88808d250000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffc9000d66fff8 CR3: 0000000043172000 CR4: 0000000000352ef0 Call Trace: <TASK> clip_push+0x6dc/0x720 net/atm/clip.c:200 clip_push+0x6dc/0x720 net/atm/clip.c:200 clip_push+0x6dc/0x720 net/atm/clip.c:200 ... clip_push+0x6dc/0x720 net/atm/clip.c:200 clip_push+0x6dc/0x720 net/atm/clip.c:200 clip_push+0x6dc/0x720 net/atm/clip.c:200 vcc_destroy_socket net/atm/common.c:183 [inline] vcc_release+0x157/0x460 net/atm/common.c:205 __sock_release net/socket.c:647 [inline] sock_close+0xc0/0x240 net/socket.c:1391 __fput+0x449/0xa70 fs/file_table.c:465 task_work_run+0x1d1/0x260 kernel/task_work.c:227 resume_user_mode_work include/linux/resume_user_mode.h:50 [inline] exit_to_user_mode_loop+0xec/0x110 kernel/entry/common.c:114 exit_to_user_mode_prepare include/linux/entry-common.h:330 [inline] syscall_exit_to_user_mode_work include/linux/entry-common.h:414 [inline] syscall_exit_to_user_mode include/linux/entry-common.h:449 [inline] do_syscall_64+0x2bd/0x3b0 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7ff31c98e929 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fffb5aa1f78 EFLAGS: 00000246 ORIG_RAX: 00000000000001b4 RAX: 0000000000000000 RBX: 0000000000012747 RCX: 00007ff31c98e929 RDX: 0000000000000000 RSI: 000000000000001e RDI: 0000000000000003 RBP: 00007ff31cbb7ba0 R08: 0000000000000001 R09: 0000000db5aa226f R10: 00007ff31c7ff030 R11: 0000000000000246 R12: 00007ff31cbb608c R13: 00007ff31cbb6080 R14: ffffffffffffffff R15: 00007fffb5aa2090 </TASK> Modules linked in:	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: atm: clip: Fix NULL pointer dereference in vcc_sendmsg() atmarpd_dev_ops does not implement the send method, which may cause crash as bellow. BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: Oops: 0010 [#1] SMP KASAN NOPTI CPU: 0 UID: 0 PID: 5324 Comm: syz.0.0 Not tainted 6.15.0-rc6-syzkaller-00346-g5723cc3450bc #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:0x0 Code: Unable to access opcode bytes at 0xffffffffffffffd6. RSP: 0018:ffffc9000d3cf778 EFLAGS: 00010246 RAX: 1fffffff1910dd1 RBX: 00000000000000c0 RCX:		

CVE-2025-38458	dffffc0000000000 RDX: ffffc9000dc82000 RSI: ffff88803e4c4640 RDI: ffff888052cd0000 RBP: ffffc9000d3cf8d0 R08: ffff888052c9143f R09: 1ffff1100a592287 R10: dffffc0000000000 R11: 0000000000000000 R12: 1ffff92001a79f00 R13: ffff888052cd0000 R14: ffff88803e4c4640 R15: ffffffff8c886e88 FS: 00007fbc762566c0(0000) GS:ffff88808d6c2000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffffffffd6 CR3: 0000000041f1b000 CR4: 0000000000352ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> vcc_sendmsg+0xa10/0xc50 net/atm/common.c:644 sock_sendmsg_nosec net/socket.c:712 [inline] __sock_sendmsg+0x219/0x270 net/socket.c:727 ____sys_sendmsg+0x52d/0x830 net/socket.c:2566 ___sys_sendmsg+0x21f/0x2a0 net/socket.c:2620 __sys_sendmmsg+0x227/0x430 net/socket.c:2709 __do_sys_sendmmsg net/socket.c:2736 [inline] __se_sys_sendmmsg net/socket.c:2733 [inline] __x64_sys_sendmmsg+0xa0/0xc0 net/socket.c:2733 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xf6/0x210 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f	N/A	More Details
CVE-2025-38457	In the Linux kernel, the following vulnerability has been resolved: net/sched: Abort __tc_modify_qdisc if parent class does not exist Lion's patch [1] revealed an ancient bug in the qdisc API. Whenever a user creates/modifies a qdisc specifying as a parent another qdisc, the qdisc API will, during grafting, detect that the user is not trying to attach to a class and reject. However grafting is performed after qdisc_create (and thus the qdiscs' init callback) is executed. In qdiscs that eventually call qdisc_tree_reduce_backlog during init or change (such as fq, hhf, choke, etc), an issue arises. For example, executing the following commands: sudo tc qdisc add dev lo root handle a: htb default 2 sudo tc qdisc add dev lo parent a: handle beef fq Qdiscs such as fq, hhf, choke, etc unconditionally invoke qdisc_tree_reduce_backlog() in their control path init() or change() which then causes a failure to find the child class; however, that does not stop the unconditional invocation of the assumed child qdisc's qlen_notify with a null class. All these qdiscs make the assumption that class is non-null. The solution is ensure that qdisc_leaf() which looks up the parent class, and is invoked prior to qdisc_create(), should return failure on not finding the class. In this patch, we leverage qdisc_leaf to return ERR_PTRs whenever the parentid doesn't correspond to a class, so that we can detect it earlier on and abort before qdisc_create is called. [1] https://lore.kernel.org/netdev/d912cbd7-193b-4269-9857-525bee8bbb6a@gmail.com/	N/A	More Details
CVE-2015-10141	An unauthenticated OS command injection vulnerability exists within Xdebug versions 2.5.5 and earlier, a PHP debugging extension developed by Derick Rethans. When remote debugging is enabled, Xdebug listens on port 9000 and accepts debugger protocol commands without authentication. An attacker can send a crafted eval command over this interface to execute arbitrary PHP code, which may invoke system-level functions such as system() or passthru(). This results in full compromise of the host under the privileges of the web server user.	N/A	More Details
CVE-2010-10012	A path traversal vulnerability exists in httpdasm version 0.92, a lightweight Windows HTTP server, that allows unauthenticated attackers to read arbitrary files on the host system. By sending a specially crafted GET request containing a sequence of URL-encoded backslashes and directory traversal patterns, an attacker can escape the web root and access sensitive files outside of the intended directory.	N/A	More Details
CVE-2025-54297	A stored XSS vulnerability in CComment component 5.0.0-6.1.14 for Joomla was discovered.	N/A	More Details
CVE-2025-54415	dag-factory is a library for Apache Airflow® to construct DAGs declaratively via configuration files. In versions 0.23.0a8 and below, a high-severity vulnerability has been identified in the cicd.yml workflow within the astronomer/dag-factory GitHub repository. The workflow, specifically when triggered by pull_request_target, is susceptible to exploitation, allowing an attacker to execute arbitrary code within the GitHub Actions runner environment. This misconfiguration enables an attacker to establish a reverse shell, exfiltrate sensitive secrets, including the highly-privileged GITHUB_TOKEN, and ultimately gain full control over the repository. This is fixed in version 0.23.0a9.	N/A	More Details
CVE-2025-38468	In the Linux kernel, the following vulnerability has been resolved: net/sched: Return NULL when htb_lookup_leaf encounters an empty rbtree htb_lookup_leaf has a BUG_ON that can trigger with the following: tc qdisc del dev lo root tc qdisc add dev lo root handle 1: htb default 1 tc class add dev lo parent 1: classid 1:1 htb rate 64bit tc qdisc add dev lo parent 1:1 handle 2: netem tc qdisc add dev lo parent 2:1 handle 3: blackhole ping -I lo -c1 -W0.001 127.0.0.1 The root cause is the following: 1. htb_dequeue calls htb_dequeue_tree which calls the dequeue handler on the selected leaf qdisc 2. netem_dequeue calls enqueue on the child qdisc 3. blackhole_enqueue drops the packet and returns a value that is not just NET_XMIT_SUCCESS 4. Because of this, netem_dequeue calls qdisc_tree_reduce_backlog, and since qlen is now 0, it calls htb_qlen_notify -> htb_deactivate -> htb_deactiviate_prios -> htb_remove_class_from_row -> htb_safe_rb_erase 5. As this is the only class in the selected hprio rbtree, __rb_change_child in __rb_erase_augmented sets the rb_root pointer to NULL 6. Because blackhole_dequeue returns NULL, netem_dequeue returns NULL, which causes htb_dequeue_tree to call htb_lookup_leaf with the same hprio rbtree, and fail the BUG_ON The function graph for this scenario is shown here: 0) | htb_enqueue() { 0) + 13.635 us | netem_enqueue(); 0) 4.719 us | htb_activate_prios(); 0) # 2249.199 us | } 0) | htb_dequeue() { 0) 2.355 us | htb_lookup_leaf(); 0) | netem_dequeue() { 0) + 11.061 us | blackhole_enqueue(); 0) | qdisc_tree_reduce_backlog() { 0) | qdisc_lookup_rcu() { 0) 1.873 us | qdisc_match_from_root(); 0) 6.292 us | } 0) 1.894 us | htb_search(); 0) | htb_qlen_notify() { 0) 2.655 us | htb_deactivate_prios(); 0) 6.933 us | } 0) + 25.227 us | } 0) 1.983 us | blackhole_dequeue(); 0) + 86.553 us | } 0) # 2932.761 us | qdisc_warn_nonwc(); 0) | htb_lookup_leaf() { 0) | BUG_ON(); --- The full original bug report can be seen here [1]. We can fix this just by returning NULL instead of the BUG_ON, as htb_dequeue_tree returns NULL when htb_lookup_leaf returns NULL. [1] https://lore.kernel.org/netdev/pF5XOOIim0IuEfhI-SOxTgRvNoDwuux7UHKnE_Y5-zVd4wmGvNk2ceHjKb8ORnzw0cGwfmVu42g9dL7XyJLf1NEzaztboTWcm0Ogxuojoeo=@willsroot.io/	N/A	More Details
CVE-2025-40730	HTML injection in Vox Media's Chorus CMS. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending them a malicious URL using the 'q' parameter in '/search'. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2024-12310	A vulnerability in Imprivata Enterprise Access Management (formerly Imprivata OneSign) allows bypassing the login screen of the shared kiosk workstation and allows unauthorized access to the underlying Windows system through the already logged-in autologon account due to insufficient handling of keyboard shortcuts. This issue affects Imprivata Enterprise Access Management versions 5.3 through 24.2.	N/A	More Details
CVE-	A sandbox escape vulnerability was identified in huggingface/smolagents version 1.14.0, allowing attackers to bypass the restricted execution environment and achieve remote code execution (RCE). The vulnerability stems from the local_python_executor.py module, which inadequately restricts Python code execution despite employing static and dynamic		More

2025-5120	checks. Attackers can exploit whitelisted modules and functions to execute arbitrary code, compromising the host system. This flaw undermines the core security boundary intended to isolate untrusted code, posing risks such as unauthorized code execution, data leakage, and potential integration-level compromise. The issue is resolved in version 1.17.0.	N/A	Details
CVE-2025-6241	LsiAgent.exe, a component of SysTrack from Lakeside Software, attempts to load several DLL files which are not present in the default installation. If a user-writable directory is present in the SYSTEM PATH environment variable, the user can write a malicious DLL to that directory with arbitrary code. This malicious DLL is executed in the context of NT AUTHORITY\SYSTEM upon service start or restart, due to the Windows default dynamic-link library search order, resulting in local elevation of privileges.	N/A	More Details
CVE-2025-50127	A SQLi vulnerability in DJ-Flyer component 1.0-3.2 for Joomla was discovered. The issue allows privileged users to execute arbitrary SQL commands.	N/A	More Details
CVE-2025-54294	A SQLi vulnerability in Komento component 4.0.0-4.0.7for Joomla was discovered. The issue allows unprivileged users to execute arbitrary SQL commands.	N/A	More Details
CVE-2025-54295	A Reflected XSS vulnerability in DJ-Reviews component 1.0-1.3.6 for Joomla was discovered.	N/A	More Details
CVE-2025-54414	Anubis is a Web AI Firewall Utility that weighs the soul of users' connections using one or more challenges in order to protect upstream resources from scraper bots. In versions 1.21.2 and below, attackers can craft malicious pass-challenge pages that cause a user to execute arbitrary JavaScript code or trigger other nonstandard schemes. An incomplete version of this fix was tagged at 1.21.2 and then the release process was aborted upon final testing. To work around this issue: block any requests to the /.within.website/x/cmd/anubis/api/pass-challenge route with the ?redir= parameter set to anything that doesn't start with the URL scheme http, https, or no scheme (local path redirect). This was fixed in version 1.21.3.	N/A	More Details
CVE-2025-8101	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability in Linkify (linkifyjs) allows XSS Targeting HTML Attributes and Manipulating User-Controlled Variables.This issue affects Linkify: from 4.3.1 before 4.3.2.	N/A	More Details
CVE-2025-54413	skops is a Python library which helps users share and ship their scikit-learn based models. Versions 0.11.0 and below contain an inconsistency in MethodNode, which can be exploited to access unexpected object fields through dot notation. This can be used to achieve arbitrary code execution at load time. While this issue may seem similar to GHSA-m7f4-hrc6-fwg3, it is actually more severe, as it relies on fewer assumptions about trusted types. This is fixed in version 12.0.0.	N/A	More Details
CVE-2025-54412	skops is a Python library which helps users share and ship their scikit-learn based models. Versions 0.11.0 and below contain a inconsistency in the OperatorFuncNode which can be exploited to hide the execution of untrusted operator methods. This can then be used in a code reuse attack to invoke seemingly safe functions and escalate to arbitrary code execution with minimal and misleading trusted types. This is fixed in version 0.12.0.	N/A	More Details
CVE-2025-54385	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions between 17.0.0-rc1 to 17.2.2 and versions 16.10.5 and below, it's possible to execute any SQL query in Oracle by using the function like DBMS_XMLGEN or DBMS_XMLQUERY. The XWiki#searchDocuments APIs pass queries directly to Hibernate without sanitization. Even when these APIs enforce a specific SELECT clause, attackers can still inject malicious code through HQL's native function support in other parts of the query (such as the WHERE clause). This is fixed in versions 16.10.6 and 17.3.0-rc-1.	N/A	More Details
CVE-2025-54296	A stored XSS vulnerability in ProFiles component 1.0-1.5.0 for Joomla was discovered.	N/A	More Details
CVE-2016-15044	A remote code execution vulnerability exists in Kaltura versions prior to 11.1.0-2 due to unsafe deserialization of user-controlled data within the keditorservices module. An unauthenticated remote attacker can exploit this issue by sending a specially crafted serialized PHP object in the kdata GET parameter to the redirectWidgetCmd endpoint. Successful exploitation leads to execution of arbitrary PHP code in the context of the web server process.	N/A	More Details
CVE-2025-50185	DbGate is cross-platform database manager. In versions 6.6.0 and below, DbGate allows unauthorized file access due to insufficient validation of file paths and types. A user with application-level access can retrieve data from arbitrary files on the system, regardless of their location or file type. The plugin fails to enforce proper checks on content type and file extension before reading a file. As a result, even sensitive files accessible only to the root user can be read through the application interface. There is currently no fix for this issue. ``` POST /runners/load-reader HTTP/1.1 Host: <REPLACE ME> User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Referer: <REPLACE ME> Content-Type: application/json Authorization: Bearer <REPLACE ME> Content-Length: 127 Origin: http://192.168.124.119:3000 Connection: keep-alive Cookie: <REPLACE ME> Priority: u=0 Cache-Control: max-age=0 {"functionName":"reader@dbgate-plugin-csv","props":{"fileName":"/etc\/shadow","limitRows":100}} ``` The request payload: ![Screenshot From 2025-05-31 22-54-49](https://github.com/user-attachments/assets/28943ad7-14f8-432a-9836-cec5c3593c0a) Lines of the file being returned: ![Screenshot From 2025-05-31 22-55-23](https://github.com/user-attachments/assets/4fae4652-097d-4d39-9f7a-6ce39346ed1d)	N/A	More Details
CVE-2025-50184	DbGate is cross-platform database manager. In versions 6.4.3-premium-beta.5 and below, DbGate is vulnerable to a directory traversal flaw. The file parameter is not properly restricted to the intended uploads directory. As a result, the endpoint that lists files within the upload directory can be manipulated to access arbitrary files on the system. By supplying a crafted path to the file parameter, an attacker can read files outside the upload directory, potentially exposing sensitive system-level data. This is fixed in version 6.4.3-beta.8.	N/A	More Details
CVE-2023-2274	Rejected reason: This CVE assignment was considered invalid after investigation.	N/A	More Details

CVE-2025-38456	In the Linux kernel, the following vulnerability has been resolved: ipmi:msghandler: Fix potential memory corruption in ipmi_create_user() The "intf" list iterator is an invalid pointer if the correct "intf->intf_num" is not found. Calling atomic_dec(&intf->nr_users) on and invalid pointer will lead to memory corruption. We don't really need to call atomic_dec() if we haven't called atomic_add_return() so update the if (intf->in_shutdown) path as well.	N/A	More Details
CVE-2025-38455	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Reject SEV{-ES} intra host migration if vCPU creation is in-flight Reject migration of SEV{-ES} state if either the source or destination VM is actively creating a vCPU, i.e. if kvm_vm_ioctl_create_vcpu() is in the section between incrementing created_vcpus and online_vcpus. The bulk of vCPU creation runs _outside_ of kvm->lock to allow creating multiple vCPUs in parallel, and so sev_info.es_active can get toggled from false=>true in the destination VM after (or during) svm_vcpu_create(), resulting in an SEV{-ES} VM effectively having a non-SEV{-ES} vCPU. The issue manifests most visibly as a crash when trying to free a vCPU's NULL VMSA page in an SEV-ES VM, but any number of things can go wrong. BUG: unable to handle page fault for address: ffffebde00000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP KASAN NOPTI CPU: 227 UID: 0 PID: 64063 Comm: syz.5.60023 Tainted: G U O 6.15.0-smp-DEV #2 NONE Tainted: [U]=USER, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 12.52.0-0 10/28/2024 RIP: 0010:constant_test_bit arch/x86/include/asm/bitops.h:206 [inline] RIP: 0010:arch_test_bit arch/x86/include/asm/bitops.h:238 [inline] RIP: 0010:_test_bit include/asm-generic/bitops/instrumented-non-atomic.h:142 [inline] RIP: 0010:PageHead include/linux/page-flags.h:866 [inline] RIP: 0010:___free_pages+0x3e/0x120 mm/page_alloc.c:5067 Code: <49> f7 06 40 00 00 00 75 05 45 31 ff eb 0c 66 90 4c 89 f0 4c 39 f0 RSP: 0018:ffff8984551978d0 EFLAGS: 00010246 RAX: 0000777f80000001 RBX: 0000000000000000 RCX: ffffffff918aeb98 RDX: 0000000000000000 RSI: 0000000000000008 RDI: ffffebde00000000 RBP: 0000000000000000 R08: ffffebde00000007 R09: 1ffffd7bc0000000 R10: dffffc0000000000 R11: fffff97bc0000001 R12: dffffc0000000000 R13: ffff8983e19751a8 R14: ffffebde00000000 R15: 1ffffd7bc0000000 FS: 0000000000000000(0000) GS:ffff89ee661d3000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffebde00000000 CR3: 000000793ceaa000 CR4: 0000000000350ef0 DR0: 0000000000000000 DR1: 0000000000000b5f DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400 Call Trace: <TASK> sev_free_vcpu+0x413/0x630 arch/x86/kvm/svm/sev.c:3169 svm_vcpu_free+0x13a/0x2a0 arch/x86/kvm/svm/svm.c:1515 kvm_arch_vcpu_destroy+0x6a/0x1d0 arch/x86/kvm/x86.c:12396 kvm_vcpu_destroy virt/kvm/kvm_main.c:470 [inline] kvm_destroy_vcpus+0xd1/0x300 virt/kvm/kvm_main.c:490 kvm_arch_destroy_vm+0x636/0x820 arch/x86/kvm/x86.c:12895 kvm_put_kvm+0xb8e/0xfb0 virt/kvm/kvm_main.c:1310 kvm_vm_release+0x48/0x60 virt/kvm/kvm_main.c:1369 __fput+0x3e4/0x9e0 fs/file_table.c:465 task_work_run+0x1a9/0x220 kernel/task_work.c:227 exit_task_work include/linux/task_work.h:40 [inline] do_exit+0x7f0/0x25b0 kernel/exit.c:953 do_group_exit+0x203/0x2d0 kernel/exit.c:1102 get_signal+0x1357/0x1480 kernel/signal.c:3034 arch_do_signal_or_restart+0x40/0x690 arch/x86/kernel/signal.c:337 exit_to_user_mode_loop kernel/entry/common.c:111 [inline] exit_to_user_mode_prepare include/linux/entry-common.h:329 [inline] __syscall_exit_to_user_mode_work kernel/entry/common.c:207 [inline] syscall_exit_to_user_mode+0x67/0xb0 kernel/entry/common.c:218 do_syscall_64+0x7c/0x150 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f87a898e969 </TASK> Modules linked in: gq(O) gsmi: Log Shutdown Reason 0x03 CR2: ffffebde00000000 ---[end trace 0000000000000000]--- Deliberately don't check for a NULL VMSA when freeing the vCPU, as crashing the host is likely desirable due to the VMSA being consumed by hardware. E.g. if KVM manages to allow VMRUN on the vCPU, hardware may read/write a bogus VMSA page. Accessing P ---truncated---	N/A	More Details
CVE-2025-38454	In the Linux kernel, the following vulnerability has been resolved: ALSA: ad1816a: Fix potential NULL pointer deref in snd_card_ad1816a_pnp() Use pr_warn() instead of dev_warn() when 'pdev' is NULL to avoid a potential NULL pointer dereference.	N/A	More Details
CVE-2014-125116	A remote code execution vulnerability exists in HybridAuth versions 2.0.9 through 2.2.2 due to insecure use of the install.php installation script. The script remains accessible after deployment and fails to sanitize input before writing to the application’s config.php file. An unauthenticated attacker can inject arbitrary PHP code into config.php, which is later executed when the file is loaded. This allows attackers to achieve remote code execution on the server. Exploitation of this issue will overwrite the existing configuration, rendering the application non-functional.	N/A	More Details
CVE-2024-13975	A local privilege escalation vulnerability exists in Commvault for Windows versions 11.20.0, 11.28.0, 11.32.0, 11.34.0, and 11.36.0. In affected configurations, a local attacker who owns a client system with the file server agent installed can compromise any assigned Windows access nodes. This may allow unauthorized access or lateral movement within the backup infrastructure. The issue has been resolved in versions 11.32.60, 11.34.34, and 11.36.8.	N/A	More Details
CVE-2022-4979	A cross-site scripting (XSS) vulnerability exists in Sitecore Experience Platform (XP) 7.5 - 10.2 and CMS 7.2 - 7.2 Update-6 that may allow authenticated Sitecore Shell users to be tricked into executing custom JS code. Managed Cloud Standard customers who run the affected Sitecore Experience Platform / CMS versions are also affected.	N/A	More Details
CVE-2020-36850	An information disclosure vulnerability exits in Sitecore JSS React Sample Application 11.0.0 - 14.0.1 that may cause page content intended for one user to be shown to another user.	N/A	More Details
CVE-2016-15046	A client-side remote code execution vulnerability exists in Hanwha Techwin SSM (Samsung Security Manager) versions 1.32 and 1.4, due to improper restrictions on the PUT method exposed by the bundled Apache ActiveMQ instance (running on port 8161). An attacker can exploit this flaw through a Cross-Origin Resource Sharing (CORS) bypass combined with JavaScript-triggered file uploads to the web server, ultimately resulting in arbitrary code execution with SYSTEM privileges. This vulnerability bypasses the server-side mitigations introduced in ZDI-15-156 and ZDI-16-481 by shifting the exploitation to the client-side. This product is now referred to as Hanwha Wisenet SSM and it is unknown if current versions are affected.	N/A	More Details
CVE-2015-10142	Sitecore Experience Platform (XP) prior to 8.0 Initial Release (rev. 141212) and Content Management System (CMS) prior to 7.2 Update-3 (rev. 141226) and prior to 7.5 Update-1 (rev. 150130) contain a vulnerability that may allow an attacker to download files under the web root of the site when the name of the file is already known via a specially-crafted URL. Affected files do not include .config, .aspx or .cs files. The issue does not allow for directory browsing.	N/A	More Details
CVE-2014-125119	A filename spoofing vulnerability exists in WinRAR when opening specially crafted ZIP archives. The issue arises due to inconsistencies between the Central Directory and Local File Header entries in ZIP files. When viewed in WinRAR, the file name from the Central Directory is displayed to the user, while the file from the Local File Header is extracted and executed. An attacker can leverage this flaw to spoof filenames and trick users into executing malicious payloads under the guise of harmless files, potentially leading to remote code execution.	N/A	More Details

CVE-2014-125118	A command injection vulnerability exists in the eScan Web Management Console version 5.5-2. The application fails to properly sanitize the 'pass' parameter when processing login requests to login.php, allowing an authenticated attacker with a valid username to inject arbitrary commands via a specially crafted password value. Successful exploitation results in remote code execution. Privilege escalation to root is possible by abusing the runasroot utility with mwconf-level privileges.	N/A	More Details
CVE-2014-125117	A stack-based buffer overflow vulnerability in the my_cgi.cgi component of certain D-Link devices, including the DSP-W215 version 1.02, can be exploited via a specially crafted HTTP POST request to the /common/info.cgi endpoint. This flaw enables an unauthenticated attacker to achieve remote code execution with system-level privileges.	N/A	More Details
CVE-2014-125115	An unauthenticated SQL injection vulnerability exists in Pandora FMS version 5.0 SP2 and earlier. The mobile/index.php endpoint fails to properly sanitize user input in the loginhash_data parameter, allowing attackers to extract administrator credentials or active session tokens via crafted requests. This occurs because input is directly concatenated into an SQL query without adequate validation, enabling SQL injection. After authentication is bypassed, a second vulnerability in the File Manager component permits arbitrary PHP file uploads. The file upload functionality does not enforce MIME-type or file extension restrictions, allowing authenticated users to upload web shells into a publicly accessible directory and achieve remote code execution.	N/A	More Details
CVE-2025-2329	In high traffic environments, a Silicon Labs OpenThread RCP (see impacted versions) fails to clear the SPI transmit buffer and may send a corrupt packet over SPI to its host, causing the host to reset the RCP which results in a denial of service.	N/A	More Details
CVE-2014-125114	A stack-based buffer overflow vulnerability exists in i-Ftp version 2.20 due to improper handling of the Time attribute within Schedule.xml. By placing a specially crafted Schedule.xml file in the i-Ftp application directory, a remote attacker can trigger a buffer overflow during scheduled download parsing, potentially leading to arbitrary code execution or a crash.	N/A	More Details
CVE-2013-10032	An authenticated remote code execution vulnerability exists in GetSimpleCMS version 3.2.1. The application’s upload.php endpoint allows authenticated users to upload arbitrary files without proper validation of MIME types or extensions. By uploading a .pht file containing PHP code, an attacker can bypass blacklist-based restrictions and place executable code within the web root. A crafted request using a polyglot or disguised extension allows the attacker to execute the payload by accessing the file directly via the web server. This vulnerability exists due to the use of a blacklist for filtering file types instead of a whitelist.	N/A	More Details
CVE-2025-38436	In the Linux kernel, the following vulnerability has been resolved: drm/scheduler: signal scheduled fence when kill job When an entity from application B is killed, drm_sched_entity_kill() removes all jobs belonging to that entity through drm_sched_entity_kill_jobs_work(). If application A's job depends on a scheduled fence from application B's job, and that fence is not properly signaled during the killing process, application A's dependency cannot be cleared. This leads to application A hanging indefinitely while waiting for a dependency that will never be resolved. Fix this issue by ensuring that scheduled fences are properly signaled when an entity is killed, allowing dependent applications to continue execution.	N/A	More Details
CVE-2025-38435	In the Linux kernel, the following vulnerability has been resolved: riscv: vector: Fix context save/restore with xtheadvector Previously only v0-v7 were correctly saved/restored, and the context of v8-v31 are damanged. Correctly save/restore v8-v31 to avoid breaking userspace.	N/A	More Details
CVE-2025-38434	In the Linux kernel, the following vulnerability has been resolved: Revert "riscv: Define TASK_SIZE_MAX for __access_ok()" This reverts commit ad5643cf2f69 ("riscv: Define TASK_SIZE_MAX for __access_ok()"). This commit changes TASK_SIZE_MAX to be LONG_MAX to optimize access_ok(), because the previous TASK_SIZE_MAX (default to TASK_SIZE) requires some computation. The reasoning was that all user addresses are less than LONG_MAX, and all kernel addresses are greater than LONG_MAX. Therefore access_ok() can filter kernel addresses. Addresses between TASK_SIZE and LONG_MAX are not valid user addresses, but access_ok() let them pass. That was thought to be okay, because they are not valid addresses at hardware level. Unfortunately, one case is missed: get_user_pages_fast() happily accepts addresses between TASK_SIZE and LONG_MAX. futex(), for instance, uses get_user_pages_fast(). This causes the problem reported by Robert [1]. Therefore, revert this commit. TASK_SIZE_MAX is changed to the default: TASK_SIZE. This unfortunately reduces performance, because TASK_SIZE is more expensive to compute compared to LONG_MAX. But correctness first, we can think about optimization later, if required.	N/A	More Details
CVE-2025-38433	In the Linux kernel, the following vulnerability has been resolved: riscv: fix runtime constant support for nommu kernels the `__runtime_fixup_32` function does not handle the case where `val` is zero correctly (as might occur when patching a nommu kernel and referring to a physical address below the 4GiB boundary whose upper 32 bits are all zero) because nothing in the existing logic prevents the code from taking the `else` branch of both nop-checks and emitting two `nop` instructions. This leaves random garbage in the register that is supposed to receive the upper 32 bits of the pointer instead of zero that when combined with the value for the lower 32 bits yields an invalid pointer and causes a kernel panic when that pointer is eventually accessed. The author clearly considered the fact that if the `lui` is converted into a `nop` that the second instruction needs to be adjusted to become an `li` instead of an `addi`, hence introducing the `addi_insn_mask` variable, but didn't follow that logic through fully to the case where the `else` branch executes. To fix it just adjust the logic to ensure that the second `else` branch is not taken if the first instruction will be patched to a `nop`.	N/A	More Details
CVE-2025-38432	In the Linux kernel, the following vulnerability has been resolved: net: netpoll: Initialize UDP checksum field before checksumming commit f1fce08e63fe ("netpoll: Eliminate redundant assignment") removed the initialization of the UDP checksum, which was wrong and broke netpoll IPv6 transmission due to bad checksumming. udph->check needs to be set before calling csum_ipv6_magic().	N/A	More Details
CVE-2025-38431	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix regression with native SMB symlinks Some users and customers reported that their backup/copy tools started to fail when the directory being copied contained symlink targets that the client couldn't parse - even when those symlinks weren't followed. Fix this by allowing lstat(2) and readlink(2) to succeed even when the client can't resolve the symlink target, restoring old behavior.	N/A	More Details
CVE-2024-13976	A DLL injection vulnerability exists in Commvault for Windows 11.20.0, 11.28.0, 11.32.0, 11.34.0, and 11.36.0. During the installation of maintenance updates, an attacker with local access may exploit uncontrolled search path or DLL loading behavior to execute arbitrary code with elevated privileges. The vulnerability has been resolved in versions 11.20.202, 11.28.124, 11.32.65, 11.34.37, and 11.36.15.	N/A	More Details
	A client-side security misconfiguration vulnerability exists in OpenBlow whistleblowing platform across multiple versions and		

CVE-2025-34114	default deployments, due to the absence of critical HTTP response headers including Content-Security-Policy, Referrer-Policy, Permissions-Policy, Cross-Origin-Embedder-Policy, and Cross-Origin-Resource-Policy. This omission weakens browser-level defenses and exposes users to cross-site scripting (XSS), clickjacking, and referer leakage. Although some instances attempt to enforce CSP via HTML <meta> tags, this method is ineffective, as modern browsers rely on header-based enforcement to reliably block inline scripts and untrusted resources.	N/A	More Details
CVE-2025-38453	In the Linux kernel, the following vulnerability has been resolved: io_uring/msg_ring: ensure io_kiocb freeing is deferred for RCU syzbot reports that defer/local task_work adding via msg_ring can hit a request that has been freed: CPU: 1 UID: 0 PID: 19356 Comm: iou-wrk-19354 Not tainted 6.16.0-rc4-syzkaller-00108-g17bbde2e1716 #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0xd2/0x2b0 mm/kasan/report.c:521 kasan_report+0x118/0x150 mm/kasan/report.c:634 io_req_local_work_add io_uring/io_uring.c:1184 [inline] __io_req_task_work_add+0x589/0x950 io_uring/io_uring.c:1252 io_msg_remote_post io_uring/msg_ring.c:103 [inline] io_msg_data_remote io_uring/msg_ring.c:133 [inline] __io_msg_ring_data+0x820/0xaa0 io_uring/msg_ring.c:151 io_msg_ring_data io_uring/msg_ring.c:173 [inline] io_msg_ring+0x134/0xa00 io_uring/msg_ring.c:314 __io_issue_sqe+0x17e/0x4b0 io_uring/io_uring.c:1739 io_issue_sqe+0x165/0xfd0 io_uring/io_uring.c:1762 io_wq_submit_work+0x6e9/0xb90 io_uring/io_uring.c:1874 io_worker_handle_work+0x7cd/0x1180 io_uring/io-wq.c:642 io_wq_worker+0x42f/0xeb0 io_uring/io-wq.c:696 ret_from_fork+0x3fc/0x770 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> which is supposed to be safe with how requests are allocated. But msg ring requests alloc and free on their own, and hence must defer freeing to a sane time. Add an rcu_head and use kfree_rcu() in both spots where requests are freed. Only the one in io_msg_tw_complete() is strictly required as it has been visible on the other ring, but use it consistently in the other spot as well. This should not cause any other issues outside of KASAN rightfully complaining about it.	N/A	More Details
CVE-2025-38444	In the Linux kernel, the following vulnerability has been resolved: raid10: cleanup memleak at raid10_make_request If raid10_read_request or raid10_write_request registers a new request and the REQ_NOWAIT flag is set, the code does not free the malloc from the mempool. unreferenced object 0xffff8884802c3200 (size 192): comm "fio", pid 9197, jiffies 4298078271 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 88 41 02 00 00 00 00 00 ....A...... 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... backtrace (crc c1a049a2): __kmalloc+0x2bb/0x450 mempool_alloc+0x11b/0x320 raid10_make_request+0x19e/0x650 [raid10] md_handle_request+0x3b3/0x9e0 __submit_bio+0x394/0x560 __submit_bio_noacct+0x145/0x530 submit_bio_noacct_nocheck+0x682/0x830 __blkdev_direct_IO_async+0x4dc/0x6b0 blkdev_read_iter+0x1e5/0x3b0 __io_read+0x230/0x1110 io_read+0x13/0x30 io_issue_sqe+0x134/0x1180 io_submit_sqes+0x48c/0xe90 __do_sys_io_uring_enter+0x574/0x8b0 do_syscall_64+0x5c/0xe0 entry_SYSCALL_64_after_hwframe+0x76/0x7e V4: changing backing tree to see if CKI tests will pass. The patch code has not changed between any versions.	N/A	More Details
CVE-2025-38452	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: rtsn: Fix a null pointer dereference in rtsn_probe() Add check for the return value of rcar_gen4_ptp_alloc() to prevent potential null pointer dereference.	N/A	More Details
CVE-2025-38451	In the Linux kernel, the following vulnerability has been resolved: md/md-bitmap: fix GPF in bitmap_get_stats() The commit message of commit 6ec1f0239485 ("md/md-bitmap: fix stats collection for external bitmaps") states: Remove the external bitmap check as the statistics should be available regardless of bitmap storage location. Return -EINVAL only for invalid bitmap with no storage (neither in superblock nor in external file). But, the code does not adhere to the above, as it does only check for a valid super-block for "internal" bitmaps. Hence, we observe: Oops: GPF, probably for non-canonical address 0x1cd66f1f40000028 RIP: 0010:bitmap_get_stats+0x45/0xd0 Call Trace: seq_read_iter+0x2b9/0x46a seq_read+0x12f/0x180 proc_reg_read+0x57/0xb0 vfs_read+0xf6/0x380 ksys_read+0x6d/0xf0 do_syscall_64+0x8c/0x1b0 entry_SYSCALL_64_after_hwframe+0x76/0x7e We fix this by checking the existence of a super-block for both the internal and external case.	N/A	More Details
CVE-2025-38450	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: prevent NULL pointer dereference in mt7925_sta_set_decap_offload() Add a NULL check for msta->vif before accessing its members to prevent a kernel panic in AP mode deployment. This also fix the issue reported in [1]. The crash occurs when this function is triggered before the station is fully initialized. The call trace shows a page fault at mt7925_sta_set_decap_offload() due to accessing resources when msta->vif is NULL. Fix this by adding an early return if msta->vif is NULL and also check wcid.sta is ready. This ensures we only proceed with decap offload configuration when the station's state is properly initialized. [14739.655703] Unable to handle kernel paging request at virtual address ffffffffffffffa0 [14739.811820] CPU: 0 UID: 0 PID: 895854 Comm: hostapd Tainted: G [14739.821394] Tainted: [C]=CRAP, [O]=OOT_MODULE [14739.825746] Hardware name: Raspberry Pi 4 Model B Rev 1.1 (DT) [14739.831577] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [14739.838538] pc : mt7925_sta_set_decap_offload+0xc0/0x1b8 [mt7925_common] [14739.845271] lr : mt7925_sta_set_decap_offload+0x58/0x1b8 [mt7925_common] [14739.851985] sp : ffffffc085efb500 [14739.855295] x29: ffffffc085efb500 x28: 0000000000000000 x27: ffffff807803a158 [14739.862436] x26: ffffff8041ececb8 x25: 0000000000000001 x24: 0000000000000001 [14739.869577] x23: 0000000000000001 x22: 0000000000000008 x21: ffffff8041ecea88 [14739.876715] x20: ffffff8041c19ca0 x19: ffffff8078031fe0 x18: 0000000000000000 [14739.883853] x17: 0000000000000000 x16: ffffffe2aeac1110 x15: 000000559da48080 [14739.890991] x14: 0000000000000001 x13: 0000000000000000 x12: 0000000000000000 [14739.898130] x11: 0a10020001008e88 x10: 0000000000001a50 x9 : ffffffe26457bfa0 [14739.905269] x8 : ffffff8042013bb0 x7 : ffffff807fb6cbf8 x6 : dead000000000100 [14739.912407] x5 : dead000000000122 x4 : ffffff80780326c8 x3 : 0000000000000000 [14739.919546] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff8041ececb8 [14739.926686] Call trace: [14739.929130] mt7925_sta_set_decap_offload+0xc0/0x1b8 [mt7925_common] [14739.935505] ieee80211_check_fast_rx+0x19c/0x510 [mac80211] [14739.941344] _sta_info_move_state+0xe4/0x510 [mac80211] [14739.946860] sta_info_move_state+0x1c/0x30 [mac80211] [14739.952116] sta_apply_auth_flags.constprop.0+0x90/0x1b0 [mac80211] [14739.958708] sta_apply_parameters+0x234/0x5e0 [mac80211] [14739.964332] ieee80211_add_station+0xdc/0x190 [mac80211] [14739.969950] nl80211_new_station+0x46c/0x670 [cfg80211] [14739.975516] genl_family_rcv_msg_doit+0xdc/0x150 [14739.980158] genl_rcv_msg+0x218/0x298 [14739.983830] netlink_rcv_skb+0x64/0x138 [14739.987670] genl_rcv+0x40/0x60 [14739.990816] netlink_unicast+0x314/0x380 [14739.994742] netlink_sendmsg+0x198/0x3f0 [14739.998664] __sock_sendmsg+0x64/0xc0 [14740.002324] ____sys_sendmsg+0x260/0x298 [14740.006242] ___sys_sendmsg+0xb4/0x110	N/A	More Details

CVE-2025-38449	In the Linux kernel, the following vulnerability has been resolved: drm/gem: Acquire references on GEM handles for framebuffers A GEM handle can be released while the GEM buffer object is attached to a DRM framebuffer. This leads to the release of the dma-buf backing the buffer object, if any. [1] Trying to use the framebuffer in further mode-setting operations leads to a segmentation fault. Most easily happens with driver that use shadow planes for vmap-ing the dma-buf during a page flip. An example is shown below. [156.791968] ------------[cut here]------------ [156.796830] WARNING: CPU: 2 PID: 2255 at drivers/dma-buf/dma-buf.c:1527 dma_buf_vmap+0x224/0x430 [...] [156.942028] RIP: 0010:dma_buf_vmap+0x224/0x430 [157.043420] Call Trace: [157.045898] <TASK> [157.048030] ? show_trace_log_lvl+0x1af/0x2c0 [157.052436] ? show_trace_log_lvl+0x1af/0x2c0 [157.056836] ? show_trace_log_lvl+0x1af/0x2c0 [157.061253] ? drm_gem_shmem_vmap+0x74/0x710 [157.065567] ? dma_buf_vmap+0x224/0x430 [157.069446] ? __warn.cold+0x58/0xe4 [157.073061] ? dma_buf_vmap+0x224/0x430 [157.077111] ? report_bug+0x1dd/0x390 [157.080842] ? handle_bug+0x5e/0xa0 [157.084389] ? exc_invalid_op+0x14/0x50 [157.088291] ? asm_exc_invalid_op+0x16/0x20 [157.092548] ? dma_buf_vmap+0x224/0x430 [157.096663] ? dma_resv_get_singleton+0x6d/0x230 [157.101341] ? __pfx_dma_buf_vmap+0x10/0x10 [157.105588] ? __pfx_dma_resv_get_singleton+0x10/0x10 [157.110697] drm_gem_shmem_vmap+0x74/0x710 [157.114866] drm_gem_vmap+0xa9/0x1b0 [157.118763] drm_gem_vmap_unlocked+0x46/0xa0 [157.123086] drm_gem_fb_vmap+0xab/0x300 [157.126979] drm_atomic_helper_prepare_planes.part.0+0x487/0xb10 [157.133032] ? lockdep_init_map_type+0x19d/0x880 [157.137701] drm_atomic_helper_commit+0x13d/0x2e0 [157.142671] ? drm_atomic_nonblocking_commit+0xa0/0x180 [157.147988] drm_mode_atomic_ioctl+0x766/0xe40 [...] [157.346424] ---[end trace 0000000000000000]--- Acquiring GEM handles for the framebuffer's GEM buffer objects prevents this from happening. The framebuffer's cleanup later puts the handle references. Commit 1a148af06000 ("drm/gem-shmem: Use dma_buf from GEM object instance") triggers the segmentation fault easily by using the dma-buf field more widely. The underlying issue with reference counting has been present before. v2: - acquire the handle instead of the BO (Christian) - fix comment style (Christian) - drop the Fixes tag (Christian) - rename err_ gotos - add missing Link tag	N/A	More Details
CVE-2025-38448	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: u_serial: Fix race condition in TTY wakeup A race condition occurs when gs_start_io() calls either gs_start_rx() or gs_start_tx(), as those functions briefly drop the port_lock for usb_ep_queue(). This allows gs_close() and gserial_disconnect() to clear port.tty and port_usb, respectively. Use the null-safe TTY Port helper function to wake up TTY. Example CPU1: CPU2: gserial_connect() // lock gs_close() // await lock gs_start_rx() // unlock usb_ep_queue() gs_close() // lock, reset port.tty and unlock gs_start_rx() // lock tty_wakeup() // NPE	N/A	More Details
CVE-2025-38447	In the Linux kernel, the following vulnerability has been resolved: mm/rmap: fix potential out-of-bounds page table access during batched unmap As pointed out by David[1], the batched unmap logic in try_to_unmap_one() may read past the end of a PTE table when a large folio's PTE mappings are not fully contained within a single page table. While this scenario might be rare, an issue triggerable from userspace must be fixed regardless of its likelihood. This patch fixes the out-of-bounds access by refactoring the logic into a new helper, folio_unmap_pte_batch(). The new helper correctly calculates the safe batch size by capping the scan at both the VMA and PMD boundaries. To simplify the code, it also supports partial batching (i.e., any number of pages from 1 up to the calculated safe maximum), as there is no strong reason to special-case for fully mapped folios.	N/A	More Details
CVE-2025-38446	In the Linux kernel, the following vulnerability has been resolved: clk: imx: Fix an out-of-bounds access in dispmix_csr_clk_dev_data When num_parents is 4, __clk_register() occurs an out-of-bounds when accessing parent_names member. Use ARRAY_SIZE() instead of hardcode number here. BUG: KASAN: global-out-of-bounds in __clk_register+0x1844/0x20d8 Read of size 8 at addr ffff800086988e78 by task kworker/u24:3/59 Hardware name: NXP i.MX95 19X19 board (DT) Workqueue: events_unbound deferred_probe_work_func Call trace: dump_backtrace+0x94/0xec show_stack+0x18/0x24 dump_stack_lvl+0x8c/0xcc print_report+0x398/0x5fc kasan_report+0xd4/0x114 __asan_report_load8_noabort+0x20/0x2c __clk_register+0x1844/0x20d8 clk_hw_register+0x44/0x110 __clk_hw_register_mux+0x284/0x3a8 imx95_bc_probe+0x4f4/0xa70	N/A	More Details
CVE-2025-38445	In the Linux kernel, the following vulnerability has been resolved: md/raid1: Fix stack memory use after return in raid1_reshape In the raid1_reshape function, newpool is allocated on the stack and assigned to conf->r1bio_pool. This results in conf->r1bio_pool.wait.head pointing to a stack address. Accessing this address later can lead to a kernel panic. Example access path: raid1_reshape() { // newpool is on the stack mempool_t newpool, oldpool; // initialize newpool.wait.head to stack address mempool_init(&newpool, ...); conf->r1bio_pool = newpool; } raid1_read_request() or raid1_write_request() { alloc_r1bio() { mempool_alloc() { // if pool->alloc fails remove_element() { --pool->curr_nr; } } } } mempool_free() { if (pool->curr_nr < pool->min_nr) { // pool->wait.head is a stack address // wake_up() will try to access this invalid address // which leads to a kernel panic return; wake_up(&pool->wait); } } Fix: reinit conf->r1bio_pool.wait after assigning newpool.	N/A	More Details
CVE-2025-38443	In the Linux kernel, the following vulnerability has been resolved: nbd: fix uaf in nbd_genl_connect() error path There is a use-after-free issue in nbd: block nbd6: Receive control failed (result -104) block nbd6: shutting down sockets == BUG: KASAN: slab-use-after-free in recv_work+0x694/0xa80 drivers/block/nbd.c:1022 Write of size 4 at addr ffff8880295de478 by task kworker/u33:0/67 CPU: 2 UID: 0 PID: 67 Comm: kworker/u33:0 Not tainted 6.15.0-rc5-syzkaller-00123-g2c89c1b655c0 #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 Workqueue: nbd6-recv recv_work Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0xc3/0x670 mm/kasan/report.c:521 kasan_report+0xe0/0x110 mm/kasan/report.c:634 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0xef/0x1a0 mm/kasan/generic.c:189 instrument_atomic_read_write include/linux/instrumented.h:96 [inline] atomic_dec include/linux/atomic/atomic-instrumented.h:592 [inline] recv_work+0x694/0xa80 drivers/block/nbd.c:1022 process_one_work+0x9cc/0x1b70 kernel/workqueue.c:3238 process_scheduled_works kernel/workqueue.c:3319 [inline] worker_thread+0x6c8/0xf10 kernel/workqueue.c:3400 kthread+0x3c2/0x780 kernel/kthread.c:464 ret_from_fork+0x45/0x80 arch/x86/kernel/process.c:153 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> nbd_genl_connect() does not properly stop the device on certain error paths after nbd_start_device() has been called. This causes the error path to put nbd->config while recv_work continue to use the config after putting it, leading to use-after-free in recv_work. This patch moves nbd_start_device() after the backend file creation.	N/A	More Details
CVE-2025-34136	An SQL injection vulnerability exists in Commvault 11.32.0 - 11.32.93, 11.36.0 - 11.36.51, and 11.38.0 - 11.38.19 Web Server component that allows a remote, unauthenticated attacker to perform SQL Injection. The vulnerability impacts systems where the CommServe and Web Server roles are installed. Other Commvault components deployed in the same environment are not affected.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: block: reject bs > ps block devices when THP is disabled If		

CVE-2025-38442	THP is disabled and when a block device with logical block size > page size is present, the following null ptr deref panic happens during boot: [[13.2 mK AOSAN: null-ptr-deref in range [0x0000000000000000-0x0000000000K0 0 0[07] [13.017749] RIP: 0010:create_empty_buffers+0x3b/0x380 <snip> [13.025448] Call Trace: [13.025692] <TASK> [13.025895] block_read_full_folio+0x610/0x780 [13.026379] ? __pfx_blkdev_get_block+0x10/0x10 [13.027008] ? __folio_batch_add_and_move+0x1fa/0x2b0 [13.027548] ? __pfx_blkdev_read_folio+0x10/0x10 [13.028080] filemap_read_folio+0x9b/0x200 [13.028526] ? __pfx_filemap_read_folio+0x10/0x10 [13.029030] ? __filemap_get_folio+0x43/0x620 [13.029497] do_read_cache_folio+0x155/0x3b0 [13.029962] ? __pfx_blkdev_read_folio+0x10/0x10 [13.030381] read_part_sector+0xb7/0x2a0 [13.030805] read_lba+0x174/0x2c0 <snip> [13.045348] nvme_scan_ns+0x684/0x850 [nvme_core] [13.045858] ? __pfx_nvme_scan_ns+0x10/0x10 [nvme_core] [13.046414] ? _raw_spin_unlock+0x15/0x40 [13.046843] ? __switch_to+0x523/0x10a0 [13.047253] ? kvm_clock_get_cycles+0x14/0x30 [13.047742] ? __pfx_nvme_scan_ns_async+0x10/0x10 [nvme_core] [13.048353] async_run_entry_fn+0x96/0x4f0 [13.048787] process_one_work+0x667/0x10a0 [13.049219] worker_thread+0x63c/0xf60 As large folio support depends on THP, only allow bs > ps block devices if THP is enabled.	N/A	More Details
CVE-2025-38441	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: account for Ethernet header in nf_flow_pppoe_proto() syzbot found a potential access to uninit-value in nf_flow_pppoe_proto() Blamed commit forgot the Ethernet header. BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x7e4/0x940 net/netfilter/nf_flow_table_inet.c:27 nf_flow_offload_inet_hook+0x7e4/0x940 net/netfilter/nf_flow_table_inet.c:27 nf_hook_entry_hookfn include/linux/netfilter.h:157 [inline] nf_hook_slow+0xe1/0x3d0 net/netfilter/core.c:623 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5742 [inline] __netif_receive_skb_core+0x4aff/0x70c0 net/core/dev.c:5837 __netif_receive_skb_one_core net/core/dev.c:5975 [inline] __netif_receive_skb+0xcc/0xac0 net/core/dev.c:6090 netif_receive_skb_internal net/core/dev.c:6176 [inline] netif_receive_skb+0x57/0x630 net/core/dev.c:6235 tun_rx_batched+0x1df/0x980 drivers/net/tun.c:1485 tun_get_user+0x4ee0/0x6b40 drivers/net/tun.c:1938 tun_chr_write_iter+0x3e9/0x5c0 drivers/net/tun.c:1984 new_sync_write fs/read_write.c:593 [inline] vfs_write+0xb4b/0x1580 fs/read_write.c:686 ksys_write fs/read_write.c:738 [inline] __do_sys_write fs/read_write.c:749 [inline]	N/A	More Details
CVE-2025-38440	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix race between DIM disable and net_dim() There's a race between disabling DIM and NAPI callbacks using the dim pointer on the RQ or SQ. If NAPI checks the DIM state bit and sees it still set, it assumes `rq->dim` or `sq->dim` is valid. But if DIM gets disabled right after that check, the pointer might already be set to NULL, leading to a NULL pointer dereference in net_dim(). Fix this by calling `synchronize_net()` before freeing the DIM context. This ensures all in-progress NAPI callbacks are finished before the pointer is cleared. Kernel log: BUG: kernel NULL pointer dereference, address: 0000000000000000 ... RIP: 0010:net_dim+0x23/0x190 ... Call Trace: <TASK> ? __die+0x20/0x60 ? page_fault_oops+0x150/0x3e0 ? common_interrupt+0xf/0xa0 ? sysvec_call_function_single+0xb/0x90 ? exc_page_fault+0x74/0x130 ? asm_exc_page_fault+0x22/0x30 ? net_dim+0x23/0x190 ? mlx5e_poll_ico_cq+0x41/0x6f0 [mlx5_core] ? sysvec_apic_timer_interrupt+0xb/0x90 mlx5e_handle_rx_dim+0x92/0xd0 [mlx5_core] mlx5e_napi_poll+0x2cd/0xac0 [mlx5_core] ? mlx5e_poll_ico_cq+0xe5/0x6f0 [mlx5_core] busy_poll_stop+0xa2/0x200 ? mlx5e_napi_poll+0x1d9/0xac0 [mlx5_core] ? mlx5e_trigger_irq+0x130/0x130 [mlx5_core] __napi_busy_loop+0x345/0x3b0 ? sysvec_call_function_single+0xb/0x90 ? asm_sysvec_call_function_single+0x16/0x20 ? sysvec_apic_timer_interrupt+0xb/0x90 ? pcpu_free_area+0x1e4/0x2e0 napi_busy_loop+0x11/0x20 xsk_recvmsg+0x10c/0x130 sock_recvmsg+0x44/0x70 __sys_recvfrom+0xbc/0x130 ? __schedule+0x398/0x890 __x64_sys_recvfrom+0x20/0x30 do_syscall_64+0x4c/0x100 entry_SYSCALL_64_after_hwframe+0x4b/0x53 ... ---[end trace 0000000000000000]--- ... ---[end Kernel panic - not syncing: Fatal exception in interrupt]---	N/A	More Details
CVE-2025-38439	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Set DMA unmap len correctly for XDP_REDIRECT When transmitting an XDP_REDIRECT packet, call dma_unmap_len_set() with the proper length instead of 0. This bug triggers this warning on a system with IOMMU enabled: WARNING: CPU: 36 PID: 0 at drivers/iommu/dma-iommu.c:842 __iommu_dma_unmap+0x159/0x170 RIP: 0010:__iommu_dma_unmap+0x159/0x170 Code: a8 00 00 00 00 48 c7 45 b0 00 00 00 00 48 c7 45 c8 00 00 00 00 48 c7 45 a0 ff ff ff ff 4c 89 45 b8 4c 89 45 c0 e9 77 ff ff ff <0f> 0b e9 60 ff ff ff e8 8b bf 6a 00 66 66 2e 0f 1f 84 00 00 00 00 RSP: 0018:ff22d31181150c88 EFLAGS: 00010206 RAX: 0000000000002000 RBX: 00000000e13a0000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ff22d31181150cf0 R08: ff22d31181150ca8 R09: 0000000000000000 R10: 0000000000000000 R11: ff22d311d36c9d80 R12: 0000000000001000 R13: ff13544d10645010 R14: ff22d31181150c90 R15: ff13544d0b2bac00 FS: 0000000000000000(0000) GS:ff13550908a00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00005be909dacff8 CR3: 0008000173408003 CR4: 0000000000f71ef0 PKRU: 55555554 Call Trace: <IRQ> ? show_regs+0x6d/0x80 ? __warn+0x89/0x160 ? __iommu_dma_unmap+0x159/0x170 ? report_bug+0x17e/0x1b0 ? handle_bug+0x46/0x90 ? exc_invalid_op+0x18/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? __iommu_dma_unmap+0x159/0x170 ? __iommu_dma_unmap+0xb3/0x170 iommu_dma_unmap_page+0x4f/0x100 dma_unmap_page_attrs+0x52/0x220 ? srso_alias_return_thunk+0x5/0xfbef5 ? xdp_return_frame+0x2e/0xd0 bnxt_tx_int_xdp+0xdf/0x440 [bnxt_en] __bnxt_poll_work_done+0x81/0x1e0 [bnxt_en] bnxt_poll+0xd3/0x1e0 [bnxt_en]	N/A	More Details
CVE-2025-38438	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: Intel: hda: Use devm_kstrdup() to avoid memleak. sof_pdata->tplg_filename can have address allocated by kstrdup() and can be overwritten. Memory leak was detected with kmemleak: unreferenced object 0xffff88812391ff60 (size 16): comm "kworker/4:1", pid 161, jiffies 4294802931 hex dump (first 16 bytes): 73 6f 66 2d 68 64 61 2d 67 65 6e 65 72 69 63 00 sof-hda-generic. backtrace (crc 4bf1675c): __kmalloc_node_track_caller_noprof+0x49c/0x6b0 kstrdup+0x46/0xc0 hda_machine_select.cold+0x1de/0x12cf [snd_sof_intel_hda_generic] sof_init_environment+0x16f/0xb50 [snd_sof] sof_probe_continue+0x45/0x7c0 [snd_sof] sof_probe_work+0x1e/0x40 [snd_sof] process_one_work+0x894/0x14b0 worker_thread+0x5e5/0xfb0 kthread+0x39d/0x760 ret_from_fork+0x31/0x70 ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2025-38437	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix potential use-after-free in oplock/lease break ack If ksmbd_iov_pin_rsp return error, use-after-free can happen by accessing opinfo->state and opinfo_put and ksmbd_fd_put could called twice.	N/A	More Details
CVE-2025-34139	A vulnerability exists in Sitecore Experience Manager (XM), Experience Platform (XP), Experience Commerce (XC), and Managed Cloud that could allow an unauthenticated attacker to read arbitrary files. This vulnerability affects all Experience Platform topologies (XM, XP, XC) from 8.0 Initial Release through 10.4 Initial Release and later. This issue affects Content Management (CM) and standalone instances. PaaS and containerized solutions are also affected.	N/A	More Details
CVE-	A vulnerability exists in Sitecore Experience Manager (XM), Experience Platform (XP), Experience Commerce (XC), and Managed		

2025-34138	Cloud that could allow remote code execution or unauthorized access to information. This vulnerability affects all Experience Platform topologies (XM, XP, XC) from 9.2 Initial Release through 10.4 Initial Release. PaaS and containerized solutions are similarly affected.	N/A	More Details
CVE-2025-43483	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The vulnerability could allow the retrieval of hardcoded cryptographic keys. HP has addressed the issue in the latest software update.	N/A	More Details