SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 July 2024

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-2024-39915	Thruk is a multibackend monitoring webinterface for Naemon, Nagios, Icinga and Shinken using the Livestatus API. This authenticated RCE in Thruk allows authorized users with network access to inject arbitrary commands via the URL parameter during PDF report generation. The Thruk web application does not properly process the url parameter when generating a PDF report. An authorized attacker with access to the reporting functionality could inject arbitrary commands that would be executed when the script /script/html2pdf.sh is called. The vulnerability can be exploited by an authorized user with network access. This issue has been addressed in version 3.16. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2024-39700	JupyterLab extension template is a `copier` template for JupyterLab extensions. Repositories created using this template with `test` option include `update-integration-tests.yml` workflow which has an RCE vulnerability. Extension authors hosting their code on GitHub are urged to upgrade the template to the latest version. Users who made changes to `update-integration-tests.yml`, accept overwriting of this file and re-apply your changes later. Users may wish to temporarily disable GitHub Actions while working on the upgrade. We recommend rebasing all open pull requests from untrusted users as actions may run using the version from the `main` branch at the time when the pull request was created. Users who are upgrading from template version prior to 4.3.0 may wish to leave out proposed changes to the release workflow for now as it requires additional configuration.	9.9	More Details
CVE-2024-6422	An unauthenticated remote attacker can manipulate the device via Telnet, stop processes, read, delete and change data.	9.8	More Details
CVE-2024-33182	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via the deviceId parameter at ip/goform/addWifiMacFilter.	9.8	More Details
CVE-2024-4879	ServiceNow has addressed an input validation vulnerability that was identified in Vancouver and Washington DC Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform. ServiceNow applied an update to hosted instances, and ServiceNow released the update to our partners and self-hosted customers. Listed below are the patches and hot fixes that address the vulnerability. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.	9.8	More Details
CVE-2024-40415	A vulnerability in /goform/SetStaticRouteCfg in the sub_519F4 function in Tenda AX1806 1.0.0.1 firmware leads to stack-based buffer overflow.	9.8	More Details
CVE-2024-40416	A vulnerability in /goform/SetVirtualServerCfg in the sub_6320C function in Tenda AX1806 1.0.0.1 firmware leads to stack-based buffer overflow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40624	TorrentPier is an open source BitTorrent Public/Private tracker engine, written in php. In `torrentpier/library/includes/functions.php`, `get_tracks()` uses the unsafe native PHP serialization format to deserialize user-controlled cookies. One can use phpggc and the chain Guzzle/FW1 to write PHP code to an arbitrary file, and execute commands on the system. For instance, the cookie bb_t will be deserialized when browsing to viewforum.php. This issue has been addressed in commit `ed37e6e52` which is expected to be included in release version 2.4.4. Users are advised to upgrade as soon as the new release is available. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2024-4143	A potential security vulnerability has been identified in certain HP PC products using AMI BIOS, which might allow arbitrary code execution. AMI has released firmware updates to mitigate this vulnerability.	9.8	More Details
CVE-2024-40524	Directory Traversal vulnerability in xmind2testcase v.1.5 allows a remote attacker to execute arbitrary code via the webtool\application.py component.	9.8	More Details
CVE-2024-6457	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the 'woof_author' parameter in all versions up to, and including, 1.3.6 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.	9.8	More Details
CVE-2024-22442	The vulnerability could be remotely exploited to bypass authentication.	9.8	More Details
CVE-2024-33180	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via the deviceId parameter at ip/goform/saveParentControlInfo.	9.8	More Details
CVE-2024-35338	Tenda i29V1.0 V1.0.0.5 was discovered to contain a hardcoded password for root.	9.8	More Details
CVE-2024-6743	AguardNet's Space Management System does not properly validate user input, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2019-16639	An issue was found on the Ruijie EG-2000 series gateway. There is a newcli.php API interface without access control, which can allow an attacker (who only has web interface access) to use TELNET commands and/or show admin passwords via the mode_url=exec&command= substring. This affects EG-2000SE EG_RGOS 11.9 B11P1.	9.8	More Details
CVE-2024-40425	File Upload vulnerability in Nanjin Xingyuantu Technology Co Sparkshop (Spark Mall B2C Mall v.1.1.6 and before allows a remote attacker to execute arbitrary code via the contorller/common.php component.	9.8	More Details
CVE-2024-40129	Open5GS v2.6.4 is vulnerable to Buffer Overflow. via /lib/pfcp/context.c.	9.8	More Details
CVE-2024-40130	open5gs v2.6.4 is vulnerable to Buffer Overflow. via /lib/core/abts.c.	9.8	More Details
CVE-2024-40392	SourceCodester Pharmacy/Medical Store Point of Sale System Using PHP/MySQL and Bootstrap Framework with Source Code 1.0 was discovered to contain a SQL injection vulnerability via the name parameter under addnew.php.	9.8	More Details
CVE-2024-40393	Online Clinic Management System In PHP With Free Source code v1.0 was discovered to contain a SQL injection vulnerability via the user parameter at login.php.	9.8	More Details
CVE-2024-40394	Simple Library Management System Project Using PHP/MySQL v1.0 was discovered to contain an arbitrary file upload vulnerability via the component ajax.php.	9.8	More Details
CVE-2024-40456	ThinkSAAS v3.7.0 was discovered to contain a SQL injection vulnerability via the name parameter at \system\action\update.php.	9.8	More Details
CVE-2024-40515	An issue in SHENZHEN TENDA TECHNOLOGY CO.,LTD Tenda AX2pro V16.03.29.48_cn allows a remote attacker to execute arbitrary code via the Routing functionality.	9.8	More Details
CVE-2024-40535	Shenzhen Libituo Technology Co., Ltd LBT-T300-T400 v3.2 was discovered to contain a stack overflow via the apn_name_3g parameter in the config_3g_para function.	9.8	More Details
CVE-2024-6744	The SMTP Listener of Secure Email Gateway from Cellopoint does not properly validate user input, leading to a Buffer Overflow vulnerability. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands on the remote server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40414	A vulnerability in /goform/SetNetControlList in the sub_656BC function in Tenda AX1806 1.0.0.1 firmware leads to stack-based buffer overflow.	9.8	More Details
CVE-2024-6624	The JSON API User plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.9.3. This is due to improper controls on custom user meta fields. This makes it possible for unauthenticated attackers to register as administrators on the site. The plugin requires the JSON API plugin to also be installed.	9.8	More Details
CVE-2024-36522	The default configuration of XSLTResourceStream.java is vulnerable to remote code execution via XSLT injection when processing input from an untrusted source without validation. Users are recommended to upgrade to versions 10.1.0, 9.18.0 or 8.16.0, which fix this issue.	9.8	More Details
CVE-2024-5217	ServiceNow has addressed an input validation vulnerability that was identified in the Washington DC, Vancouver, and earlier Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform. The vulnerability is addressed in the listed patches and hot fixes below, which were released during the June 2024 patching cycle. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.	9.8	More Details
CVE-2024-37113	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	9.8	More Details
CVE-2024-5910	Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition. Note: Expedition is a tool aiding in configuration migration, tuning, and enrichment. Configuration secrets, credentials, and other data imported into Expedition is at risk due to this issue.	9.8	More Details
CVE-2024-25077	An issue was discovered on Renesas SmartBond DA14691, DA14695, DA14697, and DA14699 devices. The Nonce used for on-the-fly decryption of flash images is stored in an unsigned header, allowing its value to be modified without invalidating the signature used for secureboot image verification. Because the encryption engine for on-the-fly decryption uses AES in CTR mode without authentication, an attacker-modified Nonce can result in execution of arbitrary code.	9.8	More Details
CVE-2024-6397	The InstaWP Connect – 1-click WP Staging & Migration plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 0.1.0.44. This is due to insufficient verification of the API key. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username, and to perform a variety of other administrative tasks. NOTE: This vulnerability was partially fixed in 0.1.0.44, but was still exploitable via Cross-Site Request Forgery.	9.8	More Details
CVE-2024-40110	Sourcecodester Poultry Farm Management System v1.0 contains an Unauthenticated Remote Code Execution (RCE) vulnerability via the productimage parameter at /farm/product.php.	9.8	More Details
CVE-2024-6407	CWE-200: Information Exposure vulnerability exists that could cause disclosure of credentials when a specially crafted message is sent to the device.	9.8	More Details
CVE-2024-36435	An issue was discovered on Supermicro BMC firmware in select X11, X12, H12, B12, X13, H13, and B13 motherboards (and CMM6 modules). An unauthenticated user can post crafted data to the interface that triggers a stack buffer overflow, and may lead to arbitrary remote code execution on a BMC.	9.8	More Details
CVE-2024-6328	The MStore API – Create Native Android & iOS Apps On The Cloud plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 4.14.7. This is due to insufficient verification on the 'phone' parameter of the 'firebase_sms_login' and 'firebase_sms_login_v2' functions. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email address or phone number. Additionally, if a new email address is supplied, a new user account is created with the default role, even if registration is disabled.	9.8	More Details
CVE-2024-21181	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2024-37927	Improper Privilege Management vulnerability in NooTheme Jobmonster allows Privilege Escalation.This issue affects Jobmonster: from n/a through 4.7.0.	9.8	More Details
CVE-2024-40539	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40542	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/role?offset.	9.8	More Details
CVE-2024-40541	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/dept/build.	9.8	More Details
CVE-2024-40540	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/dept.	9.8	More Details
CVE-2024-39914	FOG is a cloning/imaging/rescue suite/inventory management system. Prior to 1.5.10.34, packages/web/lib/fog/reportmaker.class.php in FOG was affected by a command injection via the filename parameter to /fog/management/export.php. This vulnerability is fixed in 1.5.10.34.	9.8	More Details
CVE-2024-40618	Whale browser before 3.26.244.21 allows an attacker to execute malicious JavaScript due to improper sanitization when processing a built-in extension.	9.6	More Details
CVE-2024-6385	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2, which allows an attacker to trigger a pipeline as another user under certain circumstances.	9.6	More Details
CVE-2024-6779	Out of bounds memory access in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2019-25154	Inappropriate implementation in iframe in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2023-4860	Inappropriate implementation in Skia in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2023-7012	Insufficient data validation in Permission Prompts in Google Chrome prior to 117.0.5938.62 allowed an attacker who convinced a user to install a malicious app to potentially perform a sandbox escape via a malicious file. (Chromium security severity: Medium)	9.6	More Details
CVE-2024-37933	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in anhvnit Woocommerce OpenPos.This issue affects Woocommerce OpenPos: from n/a through 6.4.4.	9.3	More Details
CVE-2024-40505	Directory Traversal vulnerability in D-Link DAP-1650 Firmware v.1.03 allows a local attacker to escalate privileges via the hedwig.cgi component.	9.3	More Details
CVE-2024-38736	Unrestricted Upload of File with Dangerous Type vulnerability in Realtyna Realtyna Organic IDX plugin allows Code Injection.This issue affects Realtyna Organic IDX plugin: from n/a through 4.14.13.	9.1	More Details
CVE-2024-37770	14Finger v1.1 was discovered to contain a remote command execution (RCE) vulnerability in the fingerprint function. This vulnerability allows attackers to execute arbitrary commands via a crafted payload.	9.1	More Details
CVE-2024-38734	Unrestricted Upload of File with Dangerous Type vulnerability in SpreadsheetConverter Import Spreadsheets from Microsoft Excel allows Code Injection.This issue affects Import Spreadsheets from Microsoft Excel: from n/a through 10.1.4.	9.1	More Details
CVE-2024-5450	The Bug Library WordPress plugin before 2.1.1 does not check the file type on user-submitted bug reports, allowing an unauthenticated user to upload PHP files	9.1	More Details
CVE-2024-37310	EVerest is an EV charging software stack. An integer overflow in the "v2g_incoming_v2gtp" function in the v2g_server.cpp implementation can allow a remote attacker to overflow the process' heap. This vulnerability is fixed in 2024.3.1 and 2024.6.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-28872	The TLS certificate validation code is flawed. An attacker can obtain a TLS certificate from the Stork server and use it to connect to the Stork agent. Once this connection is established with the valid certificate, the attacker can send malicious commands to a monitored service (Kea or BIND 9), possibly resulting in confidential data loss and/or denial of service. It should be noted that this vulnerability is not related to BIND 9 or Kea directly, and only customers using the Stork management tool are potentially affected. This issue affects Stork versions 0.15.0 through 1.15.0.	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21417	Windows Text Services Framework Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-40520	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_config_mark.php directly splicing and writing the user input data into inc_photowatermark_config.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions.	8.8	More Details
CVE-2024-40552	PublicCMS v4.0.202302.e was discovered to contain a remote commande execution (RCE) vulnerability via the cmdarray parameter at /site/ScriptComponent.java.	8.8	More Details
CVE-2024-40551	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/doUpload of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-40550	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/savePlaceMetaData of Public CMS v.4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-40548	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/save of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-40546	An arbitrary file upload vulnerability in the component /admin/cmsWebFile/save of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-40545	An arbitrary file upload vulnerability in the component /admin/cmsWebFile/doUpload of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-40544	PublicCMS v4.0.202302.e was discovered to contain a Server-Side Request Forgery (SSRF) via the component /admin/#maintenance_sysTask/edit.	8.8	More Details
CVE-2024-40543	PublicCMS v4.0.202302.e was discovered to contain a Server-Side Request Forgery (SSRF) via the component /admin/ueditor?action=catchimage.	8.8	More Details
CVE-2024-40522	There is a remote code execution vulnerability in SeaCMS 12.9. The vulnerability is caused by phomebak.php writing some variable names passed in without filtering them before writing them into the php file. An authenticated attacker can exploit this vulnerability to execute arbitrary commands and obtain system permissions.	8.8	More Details
CVE-2024-40521	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is due to the fact that although admin_template.php imposes certain restrictions on the edited file, attackers can still bypass the restrictions and write code in some way, allowing authenticated attackers to exploit the vulnerability to execute arbitrary commands and gain system privileges.	8.8	More Details
CVE-2024-40519	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_smtp.php directly splicing and writing the user input data into weixin.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions.	8.8	More Details
CVE-2024-6148	Bypass of GACS Policy Configuration settings in Citrix Workspace app for HTML5	8.8	More Details
CVE-2024-40518	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_weixin.php directly splicing and writing the user input data into weixin.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions.	8.8	More Details
CVE-2024-5325	The Form Vibes plugin for WordPress is vulnerable to SQL Injection via the ‘fv_export_data’ parameter in all versions up to, and including, 1.4.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39340	The authentication system of Securepoint UTM mishandles OTP keys. This allows the bypassing of second-factor verification (when OTP is enabled) in both the administration web interface and the user portal. Affected versions include UTM 11.5 through 12.6.4 and Reseller Preview 12.7.0. The issue has been fixed in UTM 12.6.5 and 12.7.1.	8.8	More Details
CVE-2024-6353	The Wallet for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'search[value]' parameter in all versions up to, and including, 1.5.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-6024	The ContentLock WordPress plugin through 1.0.3 does not have CSRF check in place when deleting groups or emails, which could allow attackers to make a logged in admin remove them via a CSRF attack	8.8	More Details
CVE-2024-6023	The ContentLock WordPress plugin through 1.0.3 does not have CSRF check in place when adding emails, which could allow attackers to make a logged in admin perform such action via a CSRF attack	8.8	More Details
CVE-2024-6022	The ContentLock WordPress plugin through 1.0.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	8.8	More Details
CVE-2024-39904	VNote is a note-taking platform. Prior to 3.18.1, a code execution vulnerability existed in VNote, which allowed an attacker to execute arbitrary programs on the victim's system. A crafted URI can be used in a note to perform this attack using file:/// as a link. For example, file:///C:/WINDOWS/system32/cmd.exe. This allows attackers to execute arbitrary programs by embedding a reference to a local executable file such as file:///C:/WINDOWS/system32/cmd.exe and file:///C:/WINDOWS/system32/calc.exe. This vulnerability can be exploited by creating and sharing specially crafted notes. An attacker could send a crafted note file and perform further attacks. This vulnerability is fixed in 3.18.1.	8.8	More Details
CVE-2024-6666	The WP ERP plugin for WordPress is vulnerable to SQL Injection via the ‘vendor_id’ parameter in all versions up to, and including, 1.13.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Accounting Manager access (erp_ac_view_sales_summary capability) and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-1845	The VikRentCar Car Rental Management System WordPress plugin before 1.3.2 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2024-30213	StoneFly Storage Concentrator (SC and SCVM) before 8.0.4.26 allows remote authenticated users to achieve Command Injection via a Ping URL, leading to remote code execution.	8.8	More Details
CVE-2024-5034	The SULly WordPress plugin before 4.3.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2024-5076	The wp-eMember WordPress plugin before 10.6.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2024-6775	Use after free in Media Stream in Google Chrome prior to 126.0.6478.182 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-3176	Out of bounds write in SwiftShader in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-3174	Inappropriate implementation in V8 in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-3173	Insufficient data validation in Updater in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3172	Insufficient data validation in DevTools in Google Chrome prior to 121.0.6167.85 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-3171	Use after free in Accessibility in Google Chrome prior to 122.0.6261.57 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-3170	Use after free in WebRTC in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-3169	Use after free in V8 in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-3168	Use after free in DevTools in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-7010	Use after free in WebRTC in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-6776	Use after free in Audio in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-6774	Use after free in Screen Capture in Google Chrome prior to 126.0.6478.182 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5080	The wp-eMember WordPress plugin before 10.6.6 does not validate files to be uploaded, which could allow admins to upload arbitrary files such as PHP on the server	8.8	More Details
CVE-2024-6773	Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-6772	Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-40516	An issue in H3C Technologies Co., Limited H3C Magic RC3000 RC3000V100R009 allows a remote attacker to execute arbitrary code via the Routing functionality.	8.8	More Details
CVE-2024-33181	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via the deviceMac parameter at ip/goform/addWifiMacFilter.	8.8	More Details
CVE-2024-40322	An issue was discovered in JFinalCMS v.5.0.0. There is a SQL injection vulnerablity via /admin/div_data/data	8.8	More Details
CVE-2023-49566	In Apache Linkis <=1.5.0, due to the lack of effective filtering of parameters, an attacker configuring malicious db2 parameters in the DataSource Manager Module will result in jndi injection. Therefore, the parameters in the DB2 URL should be blacklisted. This attack requires the attacker to obtain an authorized account from Linkis before it can be carried out. Versions of Apache Linkis <=1.5.0 will be affected. We recommend users upgrade the version of Linkis to version 1.6.0.	8.8	More Details
CVE-2023-46801	In Apache Linkis <= 1.5.0, data source management module, when adding Mysql data source, exists remote code execution vulnerability for java version < 1.8.0_241. The deserialization vulnerability exploited through jrmp can inject malicious files into the server and execute them. This attack requires the attacker to obtain an authorized account from Linkis before it can be carried out. We recommend that users upgrade the java version to >= 1.8.0_241. Or users upgrade Linkis to version 1.6.0.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6075	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2024-5630	The Insert or Embed Articulate Content into WordPress plugin before 4.3000000024 does not prevent authors from uploading arbitrary files to the site, which may allow them to upload PHP shells on affected sites.	8.8	More Details
CVE-2024-6737	The access control in the Electronic Official Document Management System from 2100 TECHNOLOGY is not properly implemented, allowing remote attackers with regular privileges to access the account settings functionality and create an administrator account.	8.8	More Details
CVE-2024-39565	An Improper Neutralization of Data within XPath Expressions ('XPath Injection') vulnerability in J-Web shipped with Juniper Networks Junos OS allows an unauthenticated, network-based attacker to execute remote commands on the target device. While an administrator is logged into a J-Web session or has previously logged in and subsequently logged out of their J-Web session, the attacker can arbitrarily execute commands on the target device with the other user's credentials. In the worst case, the attacker will have full control over the device. This issue affects Junos OS: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S7, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S1, 23.4R2.	8.8	More Details
CVE-2024-40549	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/savePlace of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-28828	Cross-Site request forgery in Checkmk < 2.3.0p8, < 2.2.0p29, < 2.1.0p45, and <= 2.0.0p39 (EOL) could lead to 1-click compromize of the site.	8.8	More Details
CVE-2024-6411	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 5.8.9. This is due to a lack of validation on user-supplied data in the 'pm_upload_image' AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update their user capabilities to Administrator.	8.8	More Details
CVE-2024-36451	Improper handling of insufficient permissions or privileges vulnerability exists in ajaxterm module of Webmin prior to 2.003. If this vulnerability is exploited, a console session may be hijacked by an unauthorized user. As a result, data within a system may be referred, a webpage may be altered, or a server may be permanently halted.	8.8	More Details
CVE-2024-28827	Incorrect permissions on the Checkmk Windows Agent's data directory in Checkmk < 2.3.0p8, < 2.2.0p29, < 2.1.0p45, and <= 2.0.0p39 (EOL) allows a local attacker to gain SYSTEM privileges.	8.8	More Details
CVE-2024-40331	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/dbBakMySQL_deal.php?mudi=backup	8.8	More Details
CVE-2024-40329	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/softBak_deal.php?mudi=backup	8.8	More Details
CVE-2024-40333	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/softBak_deal.php?mudi=del&dataID=2	8.8	More Details
CVE-2024-40334	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/serverFile_deal.php?mudi=upFileDel&dataID=3	8.8	More Details
CVE-2024-5792	The Houzez CRM plugin for WordPress is vulnerable to time-based SQL Injection via the notes ‘belong_to’ parameter in all versions up to, and including, 1.4.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Custom-level (seller) access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-40332	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/moneyRecord_deal.php?mudi=delRecord	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7061	The Advanced File Manager Shortcodes plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to, and including, 2.5.3. This makes it possible for authenticated attackers with contributor access or above to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2023-7062	The Advanced File Manager Shortcodes plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.4. This makes it possible for attackers with contributor access or higher to read the contents of arbitrary files on the server, which can contain sensitive information.	8.8	More Details
CVE-2024-37932	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in anhvnit Woocommerce OpenPos allows File Manipulation.This issue affects Woocommerce OpenPos: from n/a through 6.4.4.	8.6	More Details
CVE-2024-39903	Solara is a pure Python, React-style framework for scaling Jupyter and web apps. A Local File Inclusion (LFI) vulnerability was identified in widgetti/solara, in version <1.35.1, which was fixed in version 1.35.1. This vulnerability arises from the application's failure to properly validate URI fragments for directory traversal sequences such as '../' when serving static files. An attacker can exploit this flaw by manipulating the fragment part of the URI to read arbitrary files on the local file system.	8.6	More Details
CVE-2024-37928	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in NooTheme Jobmonster allows File Manipulation.This issue affects Jobmonster: from n/a through 4.7.0.	8.6	More Details
CVE-2024-21136	Vulnerability in the Oracle Retail Xstore Office product of Oracle Retail Applications (component: Security). Supported versions that are affected are 19.0.5, 20.0.3, 20.0.4, 22.0.0 and 23.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Office. While the vulnerability is in Oracle Retail Xstore Office, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Xstore Office accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	8.6	More Details
CVE-2024-22280	VMware Aria Automation does not apply correct input validation which allows for SQL-injection in the product. An authenticated malicious user could enter specially crafted SQL queries and perform unauthorised read/write operations in the database.	8.5	More Details
CVE-2024-21513	Versions of the package langchain-experimental from 0.0.15 and before 0.0.21 are vulnerable to Arbitrary Code Execution when retrieving values from the database, the code will attempt to call 'eval' on all values. An attacker can exploit this vulnerability and execute arbitrary python code if they can control the input prompt and the server is configured with VectorSQLDatabaseChain. **Notes:** Impact on the Confidentiality, Integrity and Availability of the vulnerable component: Confidentiality: Code execution happens within the impacted component, in this case langchain-experimental, so all resources are necessarily accessible. Integrity: There is nothing protected by the impacted component inherently. Although anything returned from the component counts as 'information' for which the trustworthiness can be compromised. Availability: The loss of availability isn't caused by the attack itself, but it happens as a result during the attacker's post-exploitation steps. Impact on the Confidentiality, Integrity and Availability of the subsequent system: As a legitimate low-privileged user of the package (PR:L) the attacker does not have more access to data owned by the package as a result of this vulnerability than they did with normal usage (e.g. can query the DB). The unintended action that one can perform by breaking out of the app environment and exfiltrating files, making remote connections etc. happens during the post exploitation phase in the subsequent system - in this case, the OS. AT:P: An attacker needs to be able to influence the input prompt, whilst the server is configured with the VectorSQLDatabaseChain plugin.	8.5	More Details
CVE-2024-37564	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PayPlus LTD PayPlus Payment Gateway.This issue affects PayPlus Payment Gateway: from n/a through 7.0.7.	8.5	More Details
CVE-2019-16641	An issue was found on the Ruijie EG-2000 series gateway. There is a buffer overflow in client.so. Consequently, an attacker can use login.php to login to any account, without providing its password. This affects EG-2000SE EG_RGOS 11.1(1)B1.	8.4	More Details
CVE-2024-21525	All versions of the package node-twain are vulnerable to Improper Check or Handling of Exceptional Conditions due to the length of the source data not being checked. Creating a new twain.TwainSDK with a productName or productFamily, manufacturer, version.info property of length >= 34 chars leads to a buffer overflow vulnerability.	8.3	More Details
CVE-2024-39927	Out-of-bounds write vulnerability exists in Ricoh MFPs and printers. If a remote attacker sends a specially crafted request to the affected products, the products may be able to cause a denial-of-service (DoS) condition and/or user's data may be destroyed.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21524	All versions of the package node-stringbuilder are vulnerable to Out-of-bounds Read due to incorrect memory length calculation, by calling ToBuffer, ToString, or CharAt on a StringBuilder object with a non-empty string value input. It's possible to return previously allocated memory, for example, by providing negative indexes, leading to an Information Disclosure.	8.2	More Details
CVE-2024-21141	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2024-21152	Vulnerability in the Oracle Process Manufacturing Financials product of Oracle E-Business Suite (component: Allocation Rules). Supported versions that are affected are 12.2.12-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Financials. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Process Manufacturing Financials accessible data as well as unauthorized access to critical data or complete access to all Oracle Process Manufacturing Financials accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-38354	CodiMD allows realtime collaborative markdown notes on all platforms. The notebook feature of Hackmd.io permits the rendering of iframe `HTML` tags with an improperly sanitized `name` attribute. This vulnerability enables attackers to perform cross-site scripting (XSS) attacks via DOM clobbering. This vulnerability is fixed in 2.5.4.	8.1	More Details
CVE-2024-21149	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Work Definition Issues). Supported versions that are affected are 12.2.11-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Asset Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21146	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: GL Accounts). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-37148	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated user can exploit a SQL injection vulnerability in some AJAX scripts to alter another user account data and take control of it. Upgrade to 10.0.16.	8.1	More Details
CVE-2023-52290	In streampark-console the list pages(e.g: application pages), users can sort page by field. This sort field is sent from the front-end to the back-end, and the SQL query is generated using this field. However, because this sort field isn't validated, there is a risk of SQL injection vulnerability. The attacker must successfully log into the system to launch an attack, which may cause data leakage. Since no data will be written, so this is a low-impact vulnerability. Mitigation: all users should upgrade to 2.1.4, Such parameters will be blocked.	8.1	More Details
CVE-2024-5167	The CM Email Registration Blacklist and Whitelist WordPress plugin before 1.4.9 does not have CSRF check when adding or deleting an item from the blacklist or whitelist, which could allow attackers to make a logged in admin add or delete settings from the blacklist or whitelist menu via a CSRF attack	8.1	More Details
CVE-2024-21153	Vulnerability in the Oracle Process Manufacturing Product Development product of Oracle E-Business Suite (component: Quality Management Specs). The supported version that is affected is 12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Product Development. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Process Manufacturing Product Development accessible data as well as unauthorized access to critical data or complete access to all Oracle Process Manufacturing Product Development accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21167	Vulnerability in the Oracle Trading Community product of Oracle E-Business Suite (component: Party Search UI). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Trading Community. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trading Community accessible data as well as unauthorized access to critical data or complete access to all Oracle Trading Community accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-40631	Plate media is an open source, rich-text editor for React. Editors that use `MediaEmbedElement` and pass custom `urlParsers` to the `useMediaState` hook may be vulnerable to XSS if a custom parser allows `javascript:`, `data:` or `vbscript:` URLs to be embedded. Editors that do not use `urlParsers` and consume the `url` property directly may also be vulnerable if the URL is not sanitised. The default parsers `parseTwitterUrl` and `parseVideoUrl` are not affected. `@udecode/plate-media` 36.0.10 resolves this issue by only allowing HTTP and HTTPS URLs during parsing. This affects only the `embed` property returned from `useMediaState`. In addition, the `url` property returned from `useMediaState` has been renamed to `unsafeUrl` to indicate that it has not been sanitised. The `url` property on `element` is also unsafe, but has not been renamed. If you're using either of these properties directly, you will still need to validate the URL yourself. Users are advised to upgrade. Users unable to upgrade should ensure that any custom `urlParsers` do not allow `javascript:`, `data:` or `vbscript:` URLs to be returned in the `url` property of their return values. If `url` is consumed directly, validate the URL protocol before passing it to the `iframe` element.	8.1	More Details
CVE-2024-37560	Improper Privilege Management vulnerability in IqbalRony WP User Switch allows Privilege Escalation.This issue affects WP User Switch: from n/a through 1.1.0.	8.0	More Details
CVE-2022-48837	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow.	7.8	More Details
CVE-2022-48851	In the Linux kernel, the following vulnerability has been resolved: staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len.	7.8	More Details
CVE-2022-48848	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Do not unregister events twice Nicolas reported that using: # trace-cmd record -e all -M 10 -p osnoise --poll Resulted in the following kernel warning: ------------[cut here]------------ WARNING: CPU: 0 PID: 1217 at kernel/tracepoint.c:404 tracepoint_probe_unregister+0x280/0x370 [...] CPU: 0 PID: 1217 Comm: trace-cmd Not tainted 5.17.0-rc6-next-20220307-nico+ #19 RIP: 0010:tracepoint_probe_unregister+0x280/0x370 [...] CR2: 00007ff919b29497 CR3: 0000000109da4005 CR4: 0000000000170ef0 Call Trace: <TASK> osnoise_workload_stop+0x36/0x90 tracing_set_tracer+0x108/0x260 tracing_set_trace_write+0x94/0xd0 ? __check_object_size.part.0+0x10a/0x150 ? selinux_file_permission+0x104/0x150 vfs_write+0xb5/0x290 ksys_write+0x5f/0xe0 do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7ff919a18127 [...] ---[end trace 0000000000000000]--- The warning complains about an attempt to unregister an unregistered tracepoint. This happens on trace-cmd because it first stops tracing, and then switches the tracer to nop. Which is equivalent to: # cd /sys/kernel/tracing/ # echo osnoise > current_tracer # echo 0 > tracing_on # echo nop > current_tracer The osnoise tracer stops the workload when no trace instance is actually collecting data. This can be caused both by disabling tracing or disabling the tracer itself. To avoid unregistering events twice, use the existing trace_osnoise_callback_enabled variable to check if the events (and the workload) are actually active before trying to deactivate them.	7.8	More Details
CVE-2022-48847	In the Linux kernel, the following vulnerability has been resolved: watch_queue: Fix filter limit check In watch_queue_set_filter(), there are a couple of places where we check that the filter type value does not exceed what the type_filter bitmap can hold. One place calculates the number of bits by: if (tf[i].type >= sizeof(wfilter->type_filter) * 8) which is fine, but the second does: if (tf[i].type >= sizeof(wfilter->type_filter) * BITS_PER_LONG) which is not. This can lead to a couple of out-of-bounds writes due to a too-large type: (1) __set_bit() on wfilter->type_filter (2) Writing more elements in wfilter->filters[] than we allocated. Fix this by just using the proper WATCH_TYPE__NR instead, which is the number of types we actually know about. The bug may cause an oops looking something like: BUG: KASAN: slab-out-of-bounds in watch_queue_set_filter+0x659/0x740 Write of size 4 at addr ffff88800d2c66bc by task watch_queue_oob/611 ... Call Trace: <TASK> dump_stack_lvl+0x45/0x59 print_address_description.constprop.0+0x1f/0x150 ... kasan_report.cold+0x7f/0x11b ... watch_queue_set_filter+0x659/0x740 ... __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae Allocated by task 611: kasan_save_stack+0x1e/0x40 __kasan_kmalloc+0x81/0xa0 watch_queue_set_filter+0x23a/0x740 __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88800d2c66a0 which belongs to the cache kmalloc-32 of size 32 The buggy address is located 28 bytes inside of 32-byte region [ffff88800d2c66a0, ffff88800d2c66c0)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41000	In the Linux kernel, the following vulnerability has been resolved: block/ioctl: prefer different overflow check Running syzkaller with the newly reintroduced signed integer overflow sanitizer shows this report: [62.982337] ----------[cut here]---------- [62.985692] cgroup: Invalid name [62.986211] UBSAN: signed-integer-overflow in ../block/ioctl.c:36:46 [62.989370] 9pnet_fd: p9_fd_create_tcp (7343): problem connecting socket to 127.0.0.1 [62.992992] 9223372036854775807 + 4095 cannot be represented in type 'long long' [62.997827] 9pnet_fd: p9_fd_create_tcp (7345): problem connecting socket to 127.0.0.1 [62.999369] random: crng reseeded on system resumption [63.000634] GUP no longer grows the stack in syz-executor.2 (7353): 20002000-20003000 (20001000) [63.000668] CPU: 0 PID: 7353 Comm: syz-executor.2 Not tainted 6.8.0-rc2-00035-gb3ef86b5a957 #1 [63.000677] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [63.000682] Call Trace: [63.000686] <TASK> [63.000731] dump_stack_lvl+0x93/0xd0 [63.000919] __get_user_pages+0x903/0xd30 [63.001030] __gup_longterm_locked+0x153e/0x1ba0 [63.001041] ? _raw_read_unlock_irqrestore+0x17/0x50 [63.001072] ? try_get_folio+0x29c/0x2d0 [63.001083] internal_get_user_pages_fast+0x1119/0x1530 [63.001109] iov_iter_extract_pages+0x23b/0x580 [63.001206] bio_iov_iter_get_pages+0x4de/0x1220 [63.001235] iomap_dio_bio_iter+0x9b6/0x1410 [63.001297] __iomap_dio_rw+0xab4/0x1810 [63.001316] iomap_dio_rw+0x45/0xa0 [63.001328] ext4_file_write_iter+0xdde/0x1390 [63.001372] vfs_write+0x599/0xbd0 [63.001394] ksys_write+0xc8/0x190 [63.001403] do_syscall_64+0xd4/0x1b0 [63.001421] ? arch_exit_to_user_mode_prepare+0x3a/0x60 [63.001479] entry_SYSCALL_64_after_hwframe+0x6f/0x77 [63.001535] RIP: 0033:0x7f7fd3ebf539 [63.001551] Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 f1 14 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 [63.001562] RSP: 002b:00007f7fd32570c8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 [63.001584] RAX: ffffffffffffffda RBX: 00007f7fd3ff3f80 RCX: 00007f7fd3ebf539 [63.001590] RDX: 4db6d1e4f7e43360 RSI: 0000000020000000 RDI: 0000000000000004 [63.001595] RBP: 00007f7fd3f1e496 R08: 0000000000000000 R09: 0000000000000000 [63.001599] R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 [63.001604] R13: 0000000000000006 R14: 00007f7fd3ff3f80 R15: 00007ffd415ad2b8 ... [63.018142] ---[end trace]--- Historically, the signed integer overflow sanitizer did not work in the kernel due to its interaction with `-fwrapv` but this has since been changed [1] in the newest version of Clang; It was re-enabled in the kernel with Commit 557f8c582a9ba8ab ("ubsan: Reintroduce signed overflow sanitizer"). Let's rework this overflow checking logic to not actually perform an overflow during the check itself, thus avoiding the UBSAN splat. [1]: https://github.com/llvm/llvm-project/pull/82432	7.8	More Details
CVE-2022-48854	In the Linux kernel, the following vulnerability has been resolved: net: arc_emac: Fix use after free in arc_mdio_probe() If bus->state is equal to MDIOBUS_ALLOCATED, mdiobus_free(bus) will free the "bus". But bus->name is still used in the next line, which will lead to a use after free. We can fix it by putting the name in a local variable and make the bus->name point to the rodata section "name",then use the name in the error message without referring to bus to avoid the uaf.	7.8	More Details
CVE-2024-39524	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: All versions before 20.4R3-S7-EVO, 21.2-EVO versions before 21.2R3-S8-EVO, 21.4-EVO versions before 21.4R3-S7-EVO, 22.2-EVO versions before 22.2R3-EVO, 22.3-EVO versions before 22.3R2-EVO, 22.4-EVO versions before 22.4R2-EVO.	7.8	More Details
CVE-2024-39523	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: * All versions before 20.4R3-S7-EVO, * 21.2-EVO versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.1-EVO versions before 22.1R3-S6-EVO, * 22.2-EVO versions before 22.2R3-EVO, * 22.3-EVO versions before 22.3R2-EVO, * 22.4-EVO versions before 22.4R2-EVO.	7.8	More Details
CVE-2024-39522	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: * 22.3-EVO versions before 22.3R2-EVO, * 22.4-EVO versions before 22.4R1-S1-EVO, 22.4R2-EVO.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39521	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: * 21.1-EVO versions 21.1R1-EVO and later before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.1-EVO versions before 22.1R3-S6-EVO, * 22.2-EVO versions before 22.2R3-EVO, * 22.3-EVO versions before 22.3R2-EVO.	7.8	More Details
CVE-2024-39520	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: * All version before 20.4R3-S6-EVO, * 21.2-EVO versions before 21.2R3-S4-EVO, * 21.4-EVO versions before 21.4R3-S6-EVO, * 22.2-EVO versions before 22.2R2-S1-EVO, 22.2R3-EVO, * 22.3-EVO versions before 22.3R2-EVO.	7.8	More Details
CVE-2024-32861	Under certain circumstances the Software House C●CURE 9000 Site Server provides insufficient protection of directories containing executables.	7.8	More Details
CVE-2023-52885	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix UAF in svc_tcp_listen_data_ready() After the listener svc_sock is freed, and before invoking svc_tcp_accept() for the established child sock, there is a window that the newsock retaining a freed listener svc_sock in sk_user_data which cloning from parent. In the race window, if data is received on the newsock, we will observe use-after-free report in svc_tcp_listen_data_ready(). Reproduce by two tasks: 1. while :; do rpc.nfsd 0 ; rpc.nfsd; done 2. while :; do echo "" | ncat -4 127.0.0.1 2049 ; done KASAN report: == BUG: KASAN: slab-use-after-free in svc_tcp_listen_data_ready+0x1cf/0x1f0 [sunrpc] Read of size 8 at addr ffff888139d96228 by task nc/102553 CPU: 7 PID: 102553 Comm: nc Not tainted 6.3.0+ #18 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: <IRQ> dump_stack_lvl+0x33/0x50 print_address_description.constprop.0+0x27/0x310 print_report+0x3e/0x70 kasan_report+0xae/0xe0 svc_tcp_listen_data_ready+0x1cf/0x1f0 [sunrpc] tcp_data_queue+0x9f4/0x20e0 tcp_rcv_established+0x666/0x1f60 tcp_v4_do_rcv+0x51c/0x850 tcp_v4_rcv+0x23fc/0x2e80 ip_protocol_deliver_rcu+0x62/0x300 ip_local_deliver_finish+0x267/0x350 ip_local_deliver+0x18b/0x2d0 ip_rcv+0x2fb/0x370 __netif_receive_skb_one_core+0x166/0x1b0 process_backlog+0x24c/0x5e0 __napi_poll+0xa2/0x500 net_rx_action+0x854/0xc90 __do_softirq+0x1bb/0x5de do_softirq+0xcb/0x100 </IRQ> <TASK> ... </TASK> Allocated by task 102371: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 __kasan_kmalloc+0x7b/0x90 svc_setup_socket+0x52/0x4f0 [sunrpc] svc_addsock+0x20d/0x400 [sunrpc] __write_ports_addfd+0x209/0x390 [nfsd] write_ports+0x239/0x2c0 [nfsd] nfsctl_transaction_write+0xac/0x110 [nfsd] vfs_write+0x1c3/0xae0 ksys_write+0xed/0x1c0 do_syscall_64+0x38/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc Freed by task 102551: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 kasan_save_free_info+0x2a/0x50 __kasan_slab_free+0x106/0x190 __kmem_cache_free+0x133/0x270 svc_xprt_free+0x1e2/0x350 [sunrpc] svc_xprt_destroy_all+0x25a/0x440 [sunrpc] nfsd_put+0x125/0x240 [nfsd] nfsd_svc+0x2cb/0x3c0 [nfsd] write_threads+0x1ac/0x2a0 [nfsd] nfsctl_transaction_write+0xac/0x110 [nfsd] vfs_write+0x1c3/0xae0 ksys_write+0xed/0x1c0 do_syscall_64+0x38/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc Fix the UAF by simply doing nothing in svc_tcp_listen_data_ready() if state != TCP_LISTEN, that will avoid dereferencing svsk for all child socket.	7.8	More Details
CVE-2022-48789	In the Linux kernel, the following vulnerability has been resolved: nvme-tcp: fix possible use-after-free in transport error_recovery work While nvme_tcp_submit_async_event_work is checking the ctrl and queue state before preparing the AER command and scheduling io_work, in order to fully prevent a race where this check is not reliable the error recovery work must flush async_event_work before continuing to destroy the admin queue after setting the ctrl state to RESETTING such that there is no race .submit_async_event and the error recovery handler itself changing the ctrl state.	7.8	More Details
CVE-2024-40996	In the Linux kernel, the following vulnerability has been resolved: bpf: Avoid splat in pskb_pull_reason syzkaller builds (CONFIG_DEBUG_NET=y) frequently trigger a debug hint in pskb_may_pull. We'd like to retain this debug check because it might hint at integer overflows and other issues (kernel code should pull headers, not huge value). In bpf case, this splat isn't interesting at all: such (nonsensical) bpf programs are typically generated by a fuzzer anyway. Do what Eric suggested and suppress such warning. For CONFIG_DEBUG_NET=n we don't need the extra check because pskb_may_pull will do the right thing: return an error without the WARN() backtrace.	7.8	More Details
CVE-2024-6689	Local Privilege Escalation in MSI-Installer in baramundi Management Agent v23.1.172.0 on Windows allows a local unprivileged user to escalate privileges to SYSTEM.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40903	In the Linux kernel, the following vulnerability has been resolved: usb: typec: tcpm: fix use-after-free case in tcpm_register_source_caps There could be a potential use-after-free case in tcpm_register_source_caps(). This could happen when: * new (say invalid) source caps are advertised * the existing source caps are unregistered * tcpm_register_source_caps() returns with an error as usb_power_delivery_register_capabilities() fails This causes port->partner_source_caps to hold on to the now freed source caps. Reset port->partner_source_caps value to NULL after unregistering existing source caps.	7.8	More Details
CVE-2024-40902	In the Linux kernel, the following vulnerability has been resolved: jfs: xattr: fix buffer overflow for invalid xattr When an xattr size is not what is expected, it is printed out to the kernel log in hex format as a form of debugging. But when that xattr size is bigger than the expected size, printing it out can cause an access off the end of the buffer. Fix this all up by properly restricting the size of the debug hex dump in the kernel log.	7.8	More Details
CVE-2024-40899	In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix slab-use-after-free in cachefiles_ondemand_get_fd() We got the following issue in a fuzz test of randomly issuing the restore command: == BUG: KASAN: slab-use-after-free in cachefiles_ondemand_daemon_read+0x609/0xab0 Write of size 4 at addr ffff888109164a80 by task ondemand-04-dae/4962 CPU: 11 PID: 4962 Comm: ondemand-04-dae Not tainted 6.8.0-rc7-dirty #542 Call Trace: kasan_report+0x94/0xc0 cachefiles_ondemand_daemon_read+0x609/0xab0 vfs_read+0x169/0xb50 ksys_read+0xf5/0x1e0 Allocated by task 626: __kmalloc+0x1df/0x4b0 cachefiles_ondemand_send_req+0x24d/0x690 cachefiles_create_tmpfile+0x249/0xb30 cachefiles_create_file+0x6f/0x140 cachefiles_look_up_object+0x29c/0xa60 cachefiles_lookup_cookie+0x37d/0xca0 fscache_cookie_state_machine+0x43c/0x1230 [...] Freed by task 626: kfree+0xf1/0x2c0 cachefiles_ondemand_send_req+0x568/0x690 cachefiles_create_tmpfile+0x249/0xb30 cachefiles_create_file+0x6f/0x140 cachefiles_look_up_object+0x29c/0xa60 cachefiles_lookup_cookie+0x37d/0xca0 fscache_cookie_state_machine+0x43c/0x1230 [...] == Following is the process that triggers the issue: mount I daemon_thread1 I daemon_thread2 ---------- cachefiles_ondemand_init_object cachefiles_ondemand_send_req REQ_A = kzalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cachefiles_ondemand_select_req cachefiles_ondemand_get_fd copy_to_user(_buffer, msg, n) process_open_req(REQ_A) ------ restore ------ cachefiles_ondemand_restore xas_for_each(&xas, req, ULONG_MAX) xas_set_mark(&xas, CACHEFILES_REQ_NEW); cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cachefiles_ondemand_select_req write(devfd, ("copen %u,%llu", msg->msg_id, size)); cachefiles_ondemand_copen xa_erase(&cache->reqs, id) complete(&REQ_A->done) kfree(REQ_A) cachefiles_ondemand_get_fd(REQ_A) fd = get_unused_fd_flags file = anon_inode_getfile fd_install(fd, file) load = (void *)REQ_A->msg.data; load->fd = fd; // load UAF !!! This issue is caused by issuing a restore command when the daemon is still alive, which results in a request being processed multiple times thus triggering a UAF. So to avoid this problem, add an additional reference count to cachefiles_req, which is held while waiting and reading, and then released when the waiting and reading is over. Note that since there is only one reference count for waiting, we need to avoid the same request being completed multiple times, so we can only complete the request if it is successfully removed from the xarray.	7.8	More Details
CVE-2024-39510	In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix slab-use-after-free in cachefiles_ondemand_daemon_read() We got the following issue in a fuzz test of randomly issuing the restore command: == BUG: KASAN: slab-use-after-free in cachefiles_ondemand_daemon_read+0xb41/0xb60 Read of size 8 at addr ffff888122e84088 by task ondemand-04-dae/963 CPU: 13 PID: 963 Comm: ondemand-04-dae Not tainted 6.8.0-dirty #564 Call Trace: kasan_report+0x93/0xc0 cachefiles_ondemand_daemon_read+0xb41/0xb60 vfs_read+0x169/0xb50 ksys_read+0xf5/0x1e0 Allocated by task 116: kmem_cache_alloc+0x140/0x3a0 cachefiles_lookup_cookie+0x140/0xcd0 fscache_cookie_state_machine+0x43c/0x1230 [...] Freed by task 792: kmem_cache_free+0xfe/0x390 cachefiles_put_object+0x241/0x480 fscache_cookie_state_machine+0x5c8/0x1230 [...] == Following is the process that triggers the issue: mount I daemon_thread1 I daemon_thread2 ---------- cachefiles_withdraw_cookie cachefiles_ondemand_clean_object(object) cachefiles_ondemand_send_req REQ_A = kzalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cachefiles_ondemand_select_req msg->object_id = req->object->ondemand->ondemand_id ------ restore ------ cachefiles_ondemand_restore xas_for_each(&xas, req, ULONG_MAX) xas_set_mark(&xas, CACHEFILES_REQ_NEW) cachefiles_daemon_read cachefiles_ondemand_daemon_read REQ_A = cachefiles_ondemand_select_req copy_to_user(_buffer, msg, n) xa_erase(&cache->reqs, id) complete(&REQ_A->done) ------ close(fd) ------ cachefiles_ondemand_fd_release cachefiles_put_object cachefiles_put_object kmem_cache_free(cachefiles_object_jar, object) REQ_A->object->ondemand->ondemand_id // object UAF !!! When we see the request within xa_lock, req->object must not have been freed yet, so grab the reference count of object before xa_unlock to avoid the above issue.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40906	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Always stop health timer during driver removal Currently, if teardown_hca fails to execute during driver removal, mlx5 does not stop the health timer. Afterwards, mlx5 continue with driver teardown. This may lead to a UAF bug, which results in page fault Oops[1], since the health timer invokes after resources were freed. Hence, stop the health monitor even if teardown_hca fails. [1] mlx5_core 0000:18:00.0: E-Switch: Unload vfs: mode(LEGACY), nvfs(0), necvfs(0), active vports(0) mlx5_core 0000:18:00.0: E-Switch: Disable: mode(LEGACY), nvfs(0), necvfs(0), active vports(0) mlx5_core 0000:18:00.0: E-Switch: Disable: mode(LEGACY), nvfs(0), necvfs(0), active vports(0) mlx5_core 0000:18:00.0: E-Switch: cleanup mlx5_core 0000:18:00.0: wait_func:1155:(pid 1967079): TEARDOWN_HCA(0x103) timeout. Will cause a leak of a command resource mlx5_core 0000:18:00.0: mlx5_function_close:1288:(pid 1967079): tear_down_hca failed, skip cleanup BUG: unable to handle page fault for address: ffffa26487064230 PGD 100c00067 P4D 100c00067 PUD 100e5a067 PMD 105ed7067 PTE 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 0 PID: 0 Comm: swapper/0 Tainted: G OE ------- --- 6.7.0-68.fc38.x86_64 #1 Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0013.121520200651 12/15/2020 RIP: 0010:ioread32be+0x34/0x60 RSP: 0018:ffffa26480003e58 EFLAGS: 00010292 RAX: ffffa26487064200 RBX: ffff9042d08161a0 RCX: ffff904c108222c0 RDX: 000000010bbf1b80 RSI: ffffffffc055ddb0 RDI: ffffa26487064230 RBP: ffff9042d08161a0 R08: 0000000000000022 R09: ffff904c108222e8 R10: 0000000000000004 R11: 0000000000000441 R12: ffffffffc055ddb0 R13: ffffa26487064200 R14: ffffa26480003f00 R15: ffff904c108222c0 FS: 0000000000000000(0000) GS:ffff904c10800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffa26487064230 CR3: 00000002c4420006 CR4: 0000000000706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x175/0x180 ? asm_exc_page_fault+0x26/0x30 ? __pfx_poll_health+0x10/0x10 [mlx5_core] ? __pfx_poll_health+0x10/0x10 [mlx5_core] ? ioread32be+0x34/0x60 mlx5_health_check_fatal_sensors+0x20/0x100 [mlx5_core] ? __pfx_poll_health+0x10/0x10 [mlx5_core] poll_health+0x42/0x230 [mlx5_core] ? __next_timer_interrupt+0xbc/0x110 ? __pfx_poll_health+0x10/0x10 [mlx5_core] call_timer_fn+0x21/0x130 ? __pfx_poll_health+0x10/0x10 [mlx5_core] __run_timers+0x222/0x2c0 run_timer_softirq+0x1d/0x40 __do_softirq+0xc9/0x2c8 __irq_exit_rcu+0xa6/0xc0 sysvec_apic_timer_interrupt+0x72/0x90 </IRQ> <TASK> asm_sysvec_apic_timer_interrupt+0x1a/0x20 RIP: 0010:cpuidle_enter_state+0xcc/0x440 ? cpuidle_enter_state+0xbd/0x440 cpuidle_enter+0x2d/0x40 do_idle+0x20d/0x270 cpu_startup_entry+0x2a/0x30 rest_init+0xd0/0xd0 arch_call_rest_init+0xe/0x30 start_kernel+0x709/0xa90 x86_64_start_reservations+0x18/0x30 x86_64_start_kernel+0x96/0xa0 secondary_startup_64_no_verify+0x18f/0x19b ---[end trace 0000000000000000]---	7.8	More Details
CVE-2024-40909	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a potential use-after-free in bpf_link_free() After commit 1a80dbcb2dba, bpf_link can be freed by link->ops->dealloc_deferred, but the code still tests and uses link->ops->dealloc afterward, which leads to a use-after-free as reported by syzbot. Actually, one of them should be sufficient, so just call one of them instead of both. Also add a WARN_ON() in case of any problematic implementation.	7.8	More Details
CVE-2024-39496	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free due to race with dev replace While loading a zone's info during creation of a block group, we can race with a device replace operation and then trigger a use-after-free on the device that was just replaced (source device of the replace operation). This happens because at btrfs_load_zone_info() we extract a device from the chunk map into a local variable and then use the device while not under the protection of the device replace rwsem. So if there's a device replace operation happening when we extract the device and that device is the source of the replace operation, we will trigger a use-after-free if before we finish using the device the replace operation finishes and frees the device. Fix this by enlarging the critical section under the protection of the device replace rwsem so that all uses of the device are done inside the critical section.	7.8	More Details
CVE-2024-39495	In the Linux kernel, the following vulnerability has been resolved: greybus: Fix use-after-free bug in gb_interface_release due to race condition. In gb_interface_create, &intf->mode_switch_completion is bound with gb_interface_mode_switch_work. Then it will be started by gb_interface_request_mode_switch. Here is the relevant code. if (!queue_work(system_long_wq, &intf->mode_switch_work)) { ... } If we call gb_interface_release to make cleanup, there may be an unfinished work. This function will call kfree to free the object "intf". However, if gb_interface_mode_switch_work is scheduled to run after kfree, it may cause use-after-free error as gb_interface_mode_switch_work will use the object "intf". The possible execution flow that may lead to the issue is as follows: CPU0 CPU1 l gb_interface_create l gb_interface_request_mode_switch gb_interface_release l kfree(intf) (free) l l gb_interface_mode_switch_work l mutex_lock(&intf->mutex) (use) Fix it by canceling the work before kfree.	7.8	More Details
CVE-2024-39494	In the Linux kernel, the following vulnerability has been resolved: ima: Fix use-after-free on a dentry's dname.name ->d_name.name can change on rename and the earlier value can be freed; there are conditions sufficient to stabilize it (->d_lock on dentry, ->d_lock on its parent, ->i_rwsem exclusive on the parent's inode, rename_lock), but none of those are met at any of the sites. Take a stable snapshot of the name instead.	7.8	More Details
CVE-2022-48778	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: gpmi: don't leak PM reference in error path If gpmi_nfc_apply_timings() fails, the PM runtime usage counter must be dropped.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48779	In the Linux kernel, the following vulnerability has been resolved: net: mscc: ocelot: fix use-after-free in ocelot_vlan_del() ocelot_vlan_member_del() will free the struct ocelot_bridge_vlan, so if this is the same as the port's pvid_vlan which we access afterwards, what we're accessing is freed memory. Fix the bug by determining whether to clear ocelot_port->pvid_vlan prior to calling ocelot_vlan_member_del().	7.8	More Details
CVE-2022-48834	In the Linux kernel, the following vulnerability has been resolved: usb: usbtmc: Fix bug in pipe direction for control transfers The syzbot fuzzer reported a minor bug in the usbtmc driver: usb 5-1: BOGUS control dir, pipe 80001e80 doesn't match bRequestType 0 WARNING: CPU: 0 PID: 3813 at drivers/usb/core/urb.c:412 usb_submit_urb+0x13a5/0x1970 drivers/usb/core/urb.c:410 Modules linked in: CPU: 0 PID: 3813 Comm: syz-executor122 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #0 ... Call Trace: <TASK> usb_start_wait_urb+0x113/0x530 drivers/usb/core/message.c:58 usb_internal_control_msg drivers/usb/core/message.c:102 [inline] usb_control_msg+0x2a5/0x4b0 drivers/usb/core/message.c:153 usbtmc_ioctl_request drivers/usb/class/usbtmc.c:1947 [inline] The problem is that usbtmc_ioctl_request() uses usb_rcvctrlpipe() for all of its transfers, whether they are in or out. It's easy to fix.	7.8	More Details
CVE-2024-5402	Unquoted Search Path or Element vulnerability in ABB Mint Workbench. A local attacker who successfully exploited this vulnerability could gain elevated privileges by inserting an executable file in the path of the affected service. This issue affects Mint Workbench I versions: from 5866 before 5868.	7.8	More Details
CVE-2022-48782	In the Linux kernel, the following vulnerability has been resolved: mctp: fix use after free Clang static analysis reports this problem route.c:425:4: warning: Use of memory after it is freed trace_mctp_key_acquire(key); ^~~~~~~~~~~~~~~~~~~~~~~~~~~~ When mctp_key_add() fails, key is freed but then is later used in trace_mctp_key_acquire(). Add an else statement to use the key only when mctp_key_add() is successful.	7.8	More Details
CVE-2022-48783	In the Linux kernel, the following vulnerability has been resolved: net: dsa: lantiq_gswip: fix use after free in gswip_remove() of_node_put(priv->ds->slave_mii_bus->dev.of_node) should be done before mdiobus_free(priv->ds->slave_mii_bus).	7.8	More Details
CVE-2022-48787	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: fix use-after-free If no firmware was present at all (or, presumably, all of the firmware files failed to parse), we end up unbinding by calling device_release_driver(), which calls remove(), which then in iwlwifi calls iwl_drv_stop(), freeing the 'drv' struct. However the new code I added will still erroneously access it after it was freed. Set 'failure=false' in this case to avoid the access, all data was already freed anyway.	7.8	More Details
CVE-2022-48788	In the Linux kernel, the following vulnerability has been resolved: nvme-rdma: fix possible use-after-free in transport error_recovery work While nvme_rdma_submit_async_event_work is checking the ctrl and queue state before preparing the AER command and scheduling io_work, in order to fully prevent a race where this check is not reliable the error recovery work must flush async_event_work before continuing to destroy the admin queue after setting the ctrl state to RESETTING such that there is no race .submit_async_event and the error recovery handler itself changing the ctrl state.	7.8	More Details
CVE-2024-40956	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Fix possible Use-After-Free in irq_process_work_list Use list_for_each_entry_safe() to allow iterating through the list and deleting the entry in the iteration process. The descriptor is freed via idxd_desc_complete() and there's a slight chance may cause issue for the list iterator when the descriptor is reused by another thread without it being deleted from the list.	7.8	More Details
CVE-2022-48791	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted TMF sas_task Currently a use-after-free may occur if a TMF sas_task is aborted before we handle the IO completion in mpi_ssp_completion(). The abort occurs due to timeout. When the timeout occurs, the SAS_TASK_STATE_ABORTED flag is set and the sas_task is freed in pm8001_exec_internal_tmf_task(). However, if the I/O completion occurs later, the I/O completion still thinks that the sas_task is available. Fix this by clearing the ccb->task if the TMF times out - the I/O completion handler does nothing if this pointer is cleared.	7.8	More Details
CVE-2022-48792	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted SSP/STP sas_task Currently a use-after-free may occur if a sas_task is aborted by the upper layer before we handle the I/O completion in mpi_ssp_completion() or mpi_sata_completion(). In this case, the following are the two steps in handling those I/O completions: - Call complete() to inform the upper layer handler of completion of the I/O. - Release driver resources associated with the sas_task in pm8001_ccb_task_free() call. When complete() is called, the upper layer may free the sas_task. As such, we should not touch the associated sas_task afterwards, but we do so in the pm8001_ccb_task_free() call. Fix by swapping the complete() and pm8001_ccb_task_free() calls ordering.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48796	In the Linux kernel, the following vulnerability has been resolved: iommu: Fix potential use-after-free during probe Kasan has reported the following use after free on dev->iommu. when a device probe fails and it is in process of freeing dev->iommu in dev_iommu_free function, a deferred_probe_work_func runs in parallel and tries to access dev->iommu->fwspec in of_iommu_configure path thus causing use after free. BUG: KASAN: use-after-free in of_iommu_configure+0xb4/0x4a4 Read of size 8 at addr ffffff87a2f1acb8 by task kworker/u16:2/153 Workqueue: events_unbound deferred_probe_work_func Call trace: dump_backtrace+0x0/0x33c show_stack+0x18/0x24 dump_stack_lvl+0x16c/0x1e0 print_address_description+0x84/0x39c __kasan_report+0x184/0x308 kasan_report+0x50/0x78 __asan_load8+0xc0/0xc4 of_iommu_configure+0xb4/0x4a4 of_dma_configure_id+0x2fc/0x4d4 platform_dma_configure+0x40/0x5c really_probe+0x1b4/0xb74 driver_probe_device+0x11c/0x228 __device_attach_driver+0x14c/0x304 bus_for_each_drv+0x124/0x1b0 __device_attach+0x25c/0x334 device_initial_probe+0x24/0x34 bus_probe_device+0x78/0x134 deferred_probe_work_func+0x130/0x1a8 process_one_work+0x4c8/0x970 worker_thread+0x5c8/0xaec kthread+0x1f8/0x220 ret_from_fork+0x10/0x18 Allocated by task 1: ____kasan_kmalloc+0xd4/0x114 __kasan_kmalloc+0x10/0x1c kmem_cache_alloc_trace+0xe4/0x3d4 __iommu_probe_device+0x90/0x394 probe_iommu_group+0x70/0x9c bus_for_each_dev+0x11c/0x19c bus_iommu_probe+0xb8/0x7d4 bus_set_iommu+0xcc/0x13c arm_smmu_bus_init+0x44/0x130 [arm_smmu] arm_smmu_device_probe+0xb88/0xc54 [arm_smmu] platform_drv_probe+0xe4/0x13c really_probe+0x2c8/0xb74 driver_probe_device+0x11c/0x228 device_driver_attach+0xf0/0x16c __driver_attach+0x80/0x320 bus_for_each_dev+0x11c/0x19c driver_attach+0x38/0x48 bus_add_driver+0x1dc/0x3a4 driver_register+0x18c/0x244 __platform_driver_register+0x88/0x9c init_module+0x64/0xff4 [arm_smmu] do_one_initcall+0x17c/0x2f0 do_init_module+0xe8/0x378 load_module+0x3f80/0x4a40 __se_sys_finit_module+0x1a0/0x1e4 __arm64_sys_finit_module+0x44/0x58 el0_svc_common+0x100/0x264 do_el0_svc+0x38/0xa4 el0_svc+0x20/0x30 el0_sync_handler+0x68/0xac el0_sync+0x160/0x180 Freed by task 1: kasan_set_track+0x4c/0x84 kasan_set_free_info+0x28/0x4c ____kasan_slab_free+0x120/0x15c __kasan_slab_free+0x18/0x28 slab_free_freelist_hook+0x204/0x2fc kfree+0xfc/0x3a4 __iommu_probe_device+0x284/0x394 probe_iommu_group+0x70/0x9c bus_for_each_dev+0x11c/0x19c bus_iommu_probe+0xb8/0x7d4 bus_set_iommu+0xcc/0x13c arm_smmu_bus_init+0x44/0x130 [arm_smmu] arm_smmu_device_probe+0xb88/0xc54 [arm_smmu] platform_drv_probe+0xe4/0x13c really_probe+0x2c8/0xb74 driver_probe_device+0x11c/0x228 device_driver_attach+0xf0/0x16c __driver_attach+0x80/0x320 bus_for_each_dev+0x11c/0x19c driver_attach+0x38/0x48 bus_add_driver+0x1dc/0x3a4 driver_register+0x18c/0x244 __platform_driver_register+0x88/0x9c init_module+0x64/0xff4 [arm_smmu] do_one_initcall+0x17c/0x2f0 do_init_module+0xe8/0x378 load_module+0x3f80/0x4a40 __se_sys_finit_module+0x1a0/0x1e4 __arm64_sys_finit_module+0x44/0x58 el0_svc_common+0x100/0x264 do_el0_svc+0x38/0xa4 el0_svc+0x20/0x30 el0_sync_handler+0x68/0xac el0_sync+0x160/0x180 Fix this by setting dev->iommu to NULL first and then freeing dev_iommu structure in dev_iommu_free function.	7.8	More Details
CVE-2022-48822	In the Linux kernel, the following vulnerability has been resolved: usb: f_fs: Fix use-after-free for epfile Consider a case where ffs_func_eps_disable is called from ffs_func_disable as part of composition switch and at the same time ffs_epfile_release get called from userspace. ffs_epfile_release will free up the read buffer and call ffs_data_closed which in turn destroys ffs->epfiles and mark it as NULL. While this was happening the driver has already initialized the local epfile in ffs_func_eps_disable which is now freed and waiting to acquire the spinlock. Once spinlock is acquired the driver proceeds with the stale value of epfile and tries to free the already freed read buffer causing use-after-free. Following is the illustration of the race: CPU1 CPU2 ffs_func_eps_disable epfiles (local copy) ffs_epfile_release ffs_data_closed if (last file closed) ffs_data_reset ffs_data_clear ffs_epfiles_destroy spin_lock dereference epfiles Fix this races by taking epfiles local copy & assigning it under spinlock and if epfiles(local) is null then update it in ffs->epfiles then finally destroy it. Extending the scope further from the race, protecting the ep related structures, and concurrent accesses.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40954	In the Linux kernel, the following vulnerability has been resolved: net: do not leave a dangling sk pointer, when socket creation fails It is possible to trigger a use-after-free by: * attaching an fentry probe to __sock_release() and the probe calling the bpf_get_socket_cookie() helper * running traceroute -I 1.1.1.1 on a freshly booted VM A KASAN enabled kernel will log something like below (decoded and stripped): == BUG: KASAN: slab-use-after-free in __sock_gen_cookie (./arch/x86/include/asm/atomic64_64.h:15 ./include/linux/atomic/atomic-arch-fallback.h:2583 ./include/linux/atomic/atomic-instrumented.h:1611 net/core/sock_diag.c:29) Read of size 8 at addr ffff888007110dd8 by task traceroute/299 CPU: 2 PID: 299 Comm: traceroute Tainted: G E 6.10.0-rc2+ #2 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.2-debian-1.16.2-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:117 (discriminator 1)) print_report (mm/kasan/report.c:378 mm/kasan/report.c:488) ? __sock_gen_cookie (./arch/x86/include/asm/atomic64_64.h:15 ./include/linux/atomic/atomic-arch-fallback.h:2583 ./include/linux/atomic/atomic-instrumented.h:1611 net/core/sock_diag.c:29) kasan_report (mm/kasan/report.c:603) ? __sock_gen_cookie (./arch/x86/include/asm/atomic64_64.h:15 ./include/linux/atomic/atomic-arch-fallback.h:2583 ./include/linux/atomic/atomic-instrumented.h:1611 net/core/sock_diag.c:29) kasan_check_range (mm/kasan/generic.c:183 mm/kasan/generic.c:189) __sock_gen_cookie (./arch/x86/include/asm/atomic64_64.h:15 ./include/linux/atomic/atomic-arch-fallback.h:2583 ./include/linux/atomic/atomic-instrumented.h:1611 net/core/sock_diag.c:29) bpf_get_socket_ptr_cookie (./arch/x86/include/asm/preempt.h:94 ./include/linux/sock_diag.h:42 net/core/filter.c:5094 net/core/filter.c:5092) bpf_prog_875642cf11f1d139___sock_release+0x6e/0x8e bpf_trampoline_6442506592+0x47/0xaf __sock_release (net/socket.c:652) __sock_create (net/socket.c:1601) ... Allocated by task 299 on cpu 2 at 78.328492s: kasan_save_stack (mm/kasan/common.c:48) kasan_save_track (mm/kasan/common.c:68) __kasan_slab_alloc (mm/kasan/common.c:312 mm/kasan/common.c:338) kmem_cache_alloc_noprof (mm/slub.c:3941 mm/slub.c:4000 mm/slub.c:4007) sk_prot_alloc (net/core/sock.c:2075) sk_alloc (net/core/sock.c:2134) inet_create (net/ipv4/af_inet.c:327 net/ipv4/af_inet.c:252) __sock_create (net/socket.c:1572) __sys_socket (net/socket.c:1660 net/socket.c:1644 net/socket.c:1706) __x64_sys_socket (net/socket.c:1718) do_syscall_64 (arch/x86/entry/common.c:52 arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Freed by task 299 on cpu 2 at 78.328502s: kasan_save_stack (mm/kasan/common.c:48) kasan_save_track (mm/kasan/common.c:68) kasan_save_free_info (mm/kasan/generic.c:582) poison_slab_object (mm/kasan/common.c:242) __kasan_slab_free (mm/kasan/common.c:256) kmem_cache_free (mm/slub.c:4437 mm/slub.c:4511) __sk_destruct (net/core/sock.c:2117 net/core/sock.c:2208) inet_create (net/ipv4/af_inet.c:397 net/ipv4/af_inet.c:252) __sock_create (net/socket.c:1572) __sys_socket (net/socket.c:1660 net/socket.c:1644 net/socket.c:1706) __x64_sys_socket (net/socket.c:1718) do_syscall_64 (arch/x86/entry/common.c:52 arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Fix this by clearing the struct socket reference in sk_common_release() to cover all protocol families create functions, which may already attached the reference to the sk object with sock_init_data().	7.8	More Details
CVE-2024-5681	CWE-20: Improper Input Validation vulnerability exists that could cause local denial-of-service, privilege escalation, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	7.8	More Details
CVE-2024-40994	In the Linux kernel, the following vulnerability has been resolved: ptp: fix integer overflow in max_vclocks_store On 32bit systems, the "4 * max" multiply can overflow. Use kcalloc() to do the allocation to prevent this.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40958	In the Linux kernel, the following vulnerability has been resolved: netns: Make get_net_ns() handle zero refcount net Syzkaller hit a warning: refcount_t: addition on 0; use-after-free. WARNING: CPU: 3 PID: 7890 at lib/refcount.c:25 refcount_warn_saturate+0xdf/0x1d0 Modules linked in: CPU: 3 PID: 7890 Comm: tun Not tainted 6.10.0-rc3-00100-gcaa4f9578aba-dirty #310 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:refcount_warn_saturate+0xdf/0x1d0 Code: 41 49 04 31 ff 89 de e8 9f 1e cd fe 84 db 75 9c e8 76 26 cd fe c6 05 b6 41 49 04 01 90 48 c7 c7 b8 8e 25 86 e8 d2 05 b5 fe 90 <0f> 0b 90 90 e9 79 ff ff ff e8 53 26 cd fe 0f b6 1 RSP: 0018:ffff8881067b7da0 EFLAGS: 00010286 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffffffff811c72ac RDX: ffff8881026a2140 RSI: ffffffff811c72b5 RDI: 0000000000000001 RBP: ffff8881067b7db0 R08: 0000000000000000 R09: 205b5d3730353139 R10: 0000000000000000 R11: 205d303938375420 R12: ffff8881086500c4 R13: ffff8881086500c4 R14: ffff8881086500b0 R15: ffff888108650040 FS: 00007f5b2961a4c0(0000) GS:ffff88823bd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055d7ed36fd18 CR3: 00000001482f6000 CR4: 00000000000006f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0xa3/0xc0 ? __warn+0xa5/0x1c0 ? refcount_warn_saturate+0xdf/0x1d0 ? report_bug+0x1fc/0x2d0 ? refcount_warn_saturate+0xdf/0x1d0 ? handle_bug+0xa1/0x110 ? exc_invalid_op+0x3c/0xb0 ? asm_exc_invalid_op+0x1f/0x30 ? __warn_printk+0xcc/0x140 ? __warn_printk+0xd5/0x140 ? refcount_warn_saturate+0xdf/0x1d0 get_net_ns+0xa4/0xc0 ? __pfx_get_net_ns+0x10/0x10 open_related_ns+0x5a/0x130 __tun_chr_ioctl+0x1616/0x2370 ? __sanitizer_cov_trace_switch+0x58/0xa0 ? __sanitizer_cov_trace_const_cmp2+0x1c/0x30 ? __pfx_tun_chr_ioctl+0x10/0x10 tun_chr_ioctl+0x2f/0x40 __x64_sys_ioctl+0x11b/0x160 x64_sys_call+0x1211/0x20d0 do_syscall_64+0x9e/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f5b28f165d7 Code: b3 66 90 48 8b 05 b1 48 2d 00 64 c7 00 26 00 00 00 48 c7 c0 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 81 48 2d 00 8 RSP: 002b:00007ffc2b59c5e8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f5b28f165d7 RDX: 0000000000000000 RSI: 00000000000054e3 RDI: 0000000000000003 RBP: 00007ffc2b59c650 R08: 00007f5b291ed8c0 R09: 00007f5b2961a4c0 R10: 0000000029690010 R11: 0000000000000246 R12: 0000000000400730 R13: 00007ffc2b59cf40 R14: 0000000000000000 R15: 0000000000000000 </TASK> Kernel panic - not syncing: kernel: panic_on_warn set ... This is trigger as below: ns0 ns1 tun_set_iff() //dev is tun0 tun->dev = dev //ip link set tun0 netns ns1 put_net() //ref is 0 __tun_chr_ioctl() //TUNGETDEVNETNS net = dev_net(tun->dev); open_related_ns(&net->ns, get_net_ns); //ns1 get_net_ns() get_net() //addition on 0 Use maybe_get_net() in get_net_ns in case net's ref is zero to fix this	7.8	More Details
CVE-2024-5795	A Denial of Service vulnerability was identified in GitHub Enterprise Server that allowed an attacker to cause unbounded resource exhaustion by sending a large payload to the Git server. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in version 3.13.1, 3.12.6, 3.11.12, 3.10.14, and 3.9.17. This vulnerability was reported via the GitHub Bug Bounty program.	7.7	More Details
CVE-2024-3232	A formula injection vulnerability exists in Tenable Identity Exposure where an authenticated remote attacker with administrative privileges could manipulate application form fields in order to trick another administrator into executing CSV payloads. - CVE-2024-3232	7.6	More Details
CVE-2024-21523	All versions of the package images are vulnerable to Denial of Service (DoS) due to providing unexpected input types to several different functions. This makes it possible to reach an assert macro, leading to a process crash. **Note:** By providing some specific integer values (like 0) to the size function, it is possible to obtain a Segmentation fault error, leading to the process crash.	7.5	More Details
CVE-2024-39530	An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis management daemon (chassisd) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an attempt is made to access specific sensors on platforms not supporting these sensors, either via GRPC or netconf, chassisd will crash and restart leading to a restart of all FPCs and thereby a complete outage. This issue affects Junos OS: * 21.4 versions from 21.4R3 before 21.4R3-S5, * 22.1 versions from 22.1R3 before 22.1R3-S4, * 22.2 versions from 22.2R2 before 22.2R3, * 22.3 versions from 22.3R1 before 22.3R2-S2, 22.3R3, * 22.4 versions from 22.4R1 before 22.4R2. This issue does not affect Junos OS versions earlier than 21.4.	7.5	More Details
CVE-2024-6468	Vault and Vault Enterprise did not properly handle requests originating from unauthorized IP addresses when the TCP listener option, proxy_protocol_behavior, was set to deny_unauthorized. When receiving a request from a source IP address that was not listed in proxy_protocol_authorized_addrs, the Vault API server would shut down and no longer respond to any HTTP requests, potentially resulting in denial of service. While this bug also affected versions of Vault up to 1.17.1 and 1.16.5, a separate regression in those release series did not allow Vault operators to configure the deny_unauthorized option, thus not allowing the conditions for the denial of service to occur. Fixed in Vault and Vault Enterprise 1.17.2, 1.16.6, and 1.15.12.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21526	All versions of the package speaker are vulnerable to Denial of Service (DoS) when providing unexpected input types to the channels property of the Speaker object makes it possible to reach an assert macro. Exploiting this vulnerability can lead to a process crash.	7.5	More Details
CVE-2024-38875	An issue was discovered in Django 4.2 before 4.2.14 and 5.0 before 5.0.7. urlize and urlizetrunc were subject to a potential denial of service attack via certain inputs with a very large number of brackets.	7.5	More Details
CVE-2024-39562	A Missing Release of Resource after Effective Lifetime vulnerability the xinetd process, responsible for spawning SSH daemon (sshd) instances, of Juniper Networks Junos OS Evolved allows an unauthenticated network-based attacker to cause a Denial of Service (DoS) by blocking SSH access for legitimate users. Continued receipt of these connections will create a sustained Denial of Service (DoS) condition. The issue is triggered when a high rate of concurrent SSH requests are received and terminated in a specific way, causing xinetd to crash, and leaving defunct sshd processes. Successful exploitation of this vulnerability blocks both SSH access as well as services which rely upon SSH, such as SFTP, and Netconf over SSH. Once the system is in this state, legitimate users will be unable to SSH to the device until service is manually restored. See WORKAROUND section below. Administrators can monitor an increase in defunct sshd processes by utilizing the CLI command: > show system processes l match sshd root 25219 30901 0 Jul16 ? 00:00:00 [sshd] <defunct> This issue affects Juniper Networks Junos OS Evolved: * All versions prior to 21.4R3-S7-EVO * 22.3-EVO versions prior to 22.3R2-S2-EVO, 22.3R3-S2-EVO; * 22.4-EVO versions prior to 22.4R3-EVO; * 23.2-EVO versions prior to 23.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved 22.1-EVO nor 22.2-EVO.	7.5	More Details
CVE-2024-21522	All versions of the package audify are vulnerable to Improper Validation of Array Index when frameSize is provided to the new OpusDecoder().decode or new OpusDecoder().decodeFloat functions it is not checked for negative values. This can lead to a process crash.	7.5	More Details
CVE-2024-21521	All versions of the package @discordjs/opus are vulnerable to Denial of Service (DoS) due to providing an input object with a property toString to several different functions. Exploiting this vulnerability could lead to a system crash.	7.5	More Details
CVE-2024-39552	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause the RPD process to crash leading to a Denial of Service (DoS). When a malformed BGP UPDATE packet is received over an established BGP session, RPD crashes and restarts. Continuous receipt of the malformed BGP UPDATE messages will create a sustained Denial of Service (DoS) condition for impacted devices. This issue affects eBGP and iBGP, in both IPv4 and IPv6 implementations. This issue requires a remote attacker to have at least one established BGP session. This issue affects: Juniper Networks Junos OS: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R2. Juniper Networks Junos OS Evolved: * All versions earlier than 21.2R3-S7; * 21.3-EVO versions earlier than 21.3R3-S5; * 21.4-EVO versions earlier than 21.4R3-S8; * 22.1-EVO versions earlier than 22.1R3-S4; * 22.2-EVO versions earlier than 22.2R3-S3; * 22.3-EVO versions earlier than 22.3R3-S2; * 22.4-EVO versions earlier than 22.4R3; * 23.2-EVO versions earlier than 23.2R2.	7.5	More Details
CVE-2024-39529	A Use of Externally-Controlled Format String vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If DNS Domain Generation Algorithm (DGA) detection or tunnel detection, and DNS-filtering traceoptions are configured, and specific valid transit DNS traffic is received this causes a PFE crash and restart, leading to a Denial of Service. This issue affects Junos OS: * All versions before 21.4R3-S6, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S3, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2.	7.5	More Details
CVE-2024-39555	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an attacker sending a specific malformed BGP update message to cause the session to reset, resulting in a Denial of Service (DoS). Continued receipt and processing of these malformed BGP update messages will create a sustained Denial of Service (DoS) condition. Upon receipt of a BGP update message over an established BGP session containing a specifically malformed tunnel encapsulation attribute, when segment routing is enabled, internal processing of the malformed attributes within the update results in improper parsing of remaining attributes, leading to session reset: BGP SEND Notification code 3 (Update Message Error) subcode 1 (invalid attribute list) Only systems with segment routing enabled are vulnerable to this issue. This issue affects eBGP and iBGP, in both IPv4 and IPv6 implementations, and requires a remote attacker to have at least one established BGP session. This issue affects: Junos OS: * All versions before 21.4R3-S8, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S3, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R1-S2, 23.4R2. Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-S3-EVO, * from 23.2-EVO before 23.2R2-S1-EVO, * from 23.4-EVO before 23.4R1-S2-EVO, 23.4R2-EVO.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39551	An Uncontrolled Resource Consumption vulnerability in the H.323 ALG (Application Layer Gateway) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 and MS-MPC/MIC, allows an unauthenticated network-based attacker to send specific packets causing traffic loss leading to Denial of Service (DoS). Continued receipt and processing of these specific packets will sustain the Denial of Service condition. The memory usage can be monitored using the below command. user@host> show usp memory segment sha data objcache jsf This issue affects SRX Series and MX Series with SPC3 and MS-MPC/MIC: * 20.4 before 20.4R3-S10, * 21.2 before 21.2R3-S6, * 21.3 before 21.3R3-S5, * 21.4 before 21.4R3-S6, * 22.1 before 22.1R3-S4, * 22.2 before 22.2R3-S2, * 22.3 before 22.3R3-S1, * 22.4 before 22.4R3, * 23.2 before 23.2R2.	7.5	More Details
CVE-2024-38536	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. A memory allocation failure due to `http.memcap` being reached leads to a NULL-ptr reference leading to a crash. Upgrade to 7.0.6.	7.5	More Details
CVE-2024-39614	An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. get_supported_language_variant() was subject to a potential denial-of-service attack when used with very long strings containing specific characters.	7.5	More Details
CVE-2024-39531	An Improper Handling of Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX 7000 Series allows a network-based, unauthenticated attacker to cause a Denial-of-Service (DoS). If a value is configured for DDoS bandwidth or burst parameters for any protocol in a queue, all protocols which share the same queue will have their bandwidth or burst value changed to the new value. If, for example, OSPF was configured with a certain bandwidth value, ISIS would also be limited to this value. So inadvertently either the control plane is open for a high level of specific traffic which was supposed to be limited to a lower value, or the limit for a certain protocol is so low that chances to succeed with a volumetric DoS attack are significantly increased. This issue affects Junos OS Evolved on ACX 7000 Series: * All versions before 21.4R3-S7-EVO, * 22.1 versions before 22.1R3-S6-EVO, * 22.2 versions before 22.2R3-S3-EVO, * 22.3 versions before 22.3R3-S3-EVO, * 22.4 versions before 22.4R3-S2-EVO, * 23.2 versions before 23.2R2-EVO, * 23.4 versions before 23.4R1-S1-EVO, 23.4R2-EVO.	7.5	More Details
CVE-2024-39549	A Missing Release of Memory after Effective Lifetime vulnerability in the routing process daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an attacker to send a malformed BGP Path attribute update which allocates memory used to log the bad path attribute. This memory is not properly freed in all circumstances, leading to a Denial of Service (DoS). Consumed memory can be freed by manually restarting Routing Protocol Daemon (rpd). Memory utilization could be monitored by: user@host> show system memory or show system monitor memory status This issue affects: Junos OS: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S8, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S3, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R1-S2, 23.4R2. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * from 21.4 before 21.4R3-S8-EVO, * from 22.2 before 22.2R3-S4-EVO, * from 22.3 before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-S3-EVO, * from 23.2 before 23.2R2-S1-EVO, * from 23.4 before 23.4R1-S2-EVO, 23.4R2-EVO.	7.5	More Details
CVE-2024-39548	An Uncontrolled Resource Consumption vulnerability in the aftmand process of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to consume memory resources, resulting in a Denial of Service (DoS) condition. The processes do not recover on their own and must be manually restarted. This issue affects both IPv4 and IPv6. Changes in memory usage can be monitored using the following CLI command: user@device> show system memory node <fpc slot>	grep evo-aftmann This issue affects Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.3 versions before 21.3R3-S5-EVO, * 21.4 versions before 21.4R3-S5-EVO, * 22.1 versions before 22.1R3-S4-EVO, * 22.2 versions before 22.2R3-S4-EVO, * 22.3 versions before 22.3R3-S3-EVO, * 22.4 versions before 22.4R2-S2-EVO, 22.4R3-EVO, * 23.2 versions before 23.2R1-S1-EVO, 23.2R2-EVO.	7.5	More Details
CVE-2024-39545	An Improper Check for Unusual or Exceptional Conditions vulnerability in the the IKE daemon (iked) of Juniper Networks Junos OS on SRX Series, MX Series with SPC3 and NFX350 allows allows an unauthenticated, network-based attacker sending specific mismatching parameters as part of the IPsec negotiation to trigger an iked crash leading to Denial of Service (DoS). This issue is applicable to all platforms that run iked. This issue affects Junos OS on SRX Series, MX Series with SPC3 and NFX350: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S7, * from 22.1 before 22.1R3-S2, * from 22.2 before 22.2R3-S1, * from 22.3 before 22.3R2-S1, 22.3R3, * from 22.4 before 22.4R1-S2, 22.4R2, 22.4R3.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39518	A Heap-based Buffer Overflow vulnerability in the telemetry sensor process (sensord) of Juniper Networks Junos OS on MX240, MX480, MX960 platforms using MPC10E causes a steady increase in memory utilization, ultimately leading to a Denial of Service (DoS). When the device is subscribed to a specific subscription on Junos Telemetry Interface, a slow memory leak occurs and eventually all resources are consumed and the device becomes unresponsive. A manual reboot of the Line Card will be required to restore the device to its normal functioning. This issue is only seen when telemetry subscription is active. The Heap memory utilization can be monitored using the following command: > show system processes extensive The following command can be used to monitor the memory utilization of the specific sensor > show system info	match sensord PID NAME MEMORY PEAK MEMORY %CPU THREAD-COUNT CORE-AFFINITY UPTIME 1986 sensord 877.57MB 877.57MB 2 4 0,2-15 7-21:41:32 This issue affects Junos OS: * from 21.2R3-S5 before 21.2R3-S7, * from 21.4R3-S4 before 21.4R3-S6, * from 22.2R3 before 22.2R3-S4, * from 22.3R2 before 22.3R3-S2, * from 22.4R1 before 22.4R3, * from 23.2R1 before 23.2R2.	7.5	More Details
CVE-2024-39542	An Improper Validation of Syntactic Correctness of Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series with MPC10/11 or LC9600, MX304, and Junos OS Evolved on ACX Series and PTX Series allows an unauthenticated, network based attacker to cause a Denial-of-Service (DoS). This issue can occur in two scenarios: 1. If a device, which is configured with SFLOW and ECMP, receives specific valid transit traffic, which is subject to sampling, the packetio process crashes, which in turn leads to an evo-aftman crash and causes the FPC to stop working until it is restarted. (This scenario is only applicable to PTX but not to ACX or MX.) 2. If a device receives a malformed CFM packet on an interface configured with CFM, the packetio process crashes, which in turn leads to an evo-aftman crash and causes the FPC to stop working until it is restarted. Please note that the CVSS score is for the formally more severe issue 1. The CVSS score for scenario 2. is: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) This issue affects Junos OS: * All versions before 21.2R3-S4, * 21.4 versions before 21.4R2, * 22.2 versions before 22.2R3-S2; Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.4 versions before 21.4R2-EVO.	7.5	More Details
CVE-2024-6778	Race in DevTools in Google Chrome prior to 126.0.6478.182 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: High)	7.5	More Details
CVE-2024-38534	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Crafted modbus traffic can lead to unlimited resource accumulation within a flow. Upgrade to 7.0.6. Set a limited stream.reassembly.depth to reduce the issue.	7.5	More Details
CVE-2024-38535	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Suricata can run out of memory when parsing crafted HTTP/2 traffic. Upgrade to 6.0.20 or 7.0.6.	7.5	More Details
CVE-2024-21183	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2024-36432	An arbitrary memory write vulnerability was discovered in Supermicro X11DPG-HGX2, X11PDG-QT, X11PDG-OT, and X11PDG-SN motherboards with BIOS firmware before 4.4.	7.5	More Details
CVE-2024-6089	An input validation vulnerability exists in the Rockwell Automation 5015 - AENFTXT when a manipulated PTP packet is sent, causing the secondary adapter to result in a major nonrecoverable fault. If exploited, a power cycle is required to recover the product.	7.5	More Details
CVE-2024-36433	An arbitrary memory write vulnerability was discovered in Supermicro X11DPH-T, X11DPH-Tq, and X11DPH-i motherboards with BIOS firmware before 4.4.	7.5	More Details
CVE-2019-16640	An issue was found in upload.php on the Ruijie EG-2000 series gateway. A parameter passed to the class UploadFile is mishandled (%00 and /var/./html are not checked), which can allow an attacker to upload any file to the gateway. This affects EG-2000SE EG_RGOS 11.9 B11P1.	7.5	More Details
CVE-2019-16638	An issue was found on the Ruijie EG-2000 series gateway. An attacker can easily dump cleartext stored passwords in /data/config.text with simple XORs. This affects EG-2000SE EG_RGOS 11.1(1)B1.	7.5	More Details
CVE-2024-36434	An SMM callout vulnerability was discovered in Supermicro X11DPH-T, X11DPH-Tq, and X11DPH-i motherboards with BIOS firmware before 4.4.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37110	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	7.5	More Details
CVE-2024-39540	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on SRX Series, and MX Series with SPC3 allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an affected device receives specific valid TCP traffic, the pfe crashes and restarts leading to a momentary but complete service outage. This issue affects Junos OS: 21.2 releases from 21.2R3-S5 before 21.2R3-S6. This issue does not affect earlier or later releases.	7.5	More Details
CVE-2024-37115	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Automattic Newspack Blocks.This issue affects Newspack Blocks: from n/a through 3.0.8.	7.5	More Details
CVE-2024-21182	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2024-40554	An access control issue in Tmall_demo v2024.07.03 allows attackers to obtain sensitive information.	7.5	More Details
CVE-2024-21175	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2024-39693	Next.js is a React framework. A Denial of Service (DoS) condition was identified in Next.js. Exploitation of the bug can trigger a crash, affecting the availability of the server. his vulnerability was resolved in Next.js 13.5 and later.	7.5	More Details
CVE-2024-38735	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in N.O.U.S. Open Useful and Simple Event post allows PHP Local File Inclusion.This issue affects Event post: from n/a through 5.9.5.	7.5	More Details
CVE-2024-6421	An unauthenticated remote attacker can read out sensitive device information through a incorrectly configured FTP service.	7.5	More Details
CVE-2024-37940	Cross-Site Request Forgery (CSRF) vulnerability in Seraphinite Solutions Seraphinite Accelerator (Full, premium).This issue affects Seraphinite Accelerator (Full, premium): from n/a through 2.21.13.	7.4	More Details
CVE-2024-21147	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	7.4	More Details
CVE-2024-6492	Exposure of Sensitive Information in edge browser session proxy feature in Devolutions Remote Desktop Manager 2024.2.14.0 and earlier on Windows allows an attacker to intercept proxy credentials via a specially crafted website.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40560	Tmall_demo before v2024.07.03 was discovered to contain a SQL injection vulnerability.	7.3	More Details
CVE-2024-36438	eLinkSmart Hidden Smart Cabinet Lock 2024-05-22 has Incorrect Access Control and fails to perform an authorization check which can lead to card duplication and other attacks.	7.3	More Details
CVE-2024-6745	A vulnerability classified as critical has been found in code-projects Simple Ticket Booking 1.0. Affected is an unknown function of the file adminauthenticate.php of the component Login. The manipulation of the argument email/password 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 identifier of this vulnerability is VDB-271476.	7.3	More Details
CVE-2024-39546	A Missing Authorization vulnerability in the Socket Intercept (SI) command file interface of Juniper Networks Junos OS Evolved allows an authenticated, low-privilege local attacker to modify certain files, allowing the attacker to cause any command to execute with root privileges leading to privilege escalation ultimately compromising the system. This issue affects Junos OS Evolved: * All versions prior to 21.2R3-S8-EVO, * 21.4 versions prior to 21.4R3-S6-EVO, * 22.1 versions prior to 22.1R3-S5-EVO, * 22.2 versions prior to 22.2R3-S3-EVO, * 22.3 versions prior to 22.3R3-S3-EVO, * 22.4 versions prior to 22.4R3-EVO, * 23.2 versions prior to 23.2R2-EVO.	7.3	More Details
CVE-2024-40626	Outline is an open source, collaborative document editor. A type confusion issue was found in ProseMirror's rendering process that leads to a Stored Cross-Site Scripting (XSS) vulnerability in Outline. An authenticated user can create a document containing a malicious JavaScript payload. When other users view this document, the malicious Javascript can execute in the origin of Outline. Outline includes CSP rules to prevent third-party code execution, however in the case of self-hosting and having your file storage on the same domain as Outline a malicious payload can be uploaded as a file attachment and bypass those CSP restrictions. This issue has been addressed in release version 0.77.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2024-6653	A vulnerability was found in code-projects Simple Task List 1.0. It has been declared as critical. This vulnerability affects unknown code of the file loginForm.php of the component Login. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271060.	7.3	More Details
CVE-2024-2602	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could result in remote code execution when an authenticated user executes a saved project file that has been tampered by a malicious actor.	7.3	More Details
CVE-2024-21184	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19.3-19.23. Easily exploitable vulnerability allows high privileged attacker having Execute on SYS.XS_DIAG privilege with network access via Oracle Net to compromise Oracle Database RDBMS Security. Successful attacks of this vulnerability can result in takeover of Oracle Database RDBMS Security. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2024-39917	xrdp is an open source RDP server. xrdp versions prior to 0.10.0 have a vulnerability that allows attackers to make an infinite number of login attempts. The number of max login attempts is supposed to be limited by a configuration parameter `MaxLoginRetry` in `/etc/xrdp/sesman.ini`. However, this mechanism was not effectively working. As a result, xrdp allows an infinite number of login attempts.	7.2	More Details
CVE-2024-5902	The User Feedback – Create Interactive Feedback Form, User Surveys, and Polls in Seconds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the name parameter in all versions up to, and including, 1.0.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in feedback form responses that will execute whenever a high-privileged user tries to view them.	7.2	More Details
CVE-2024-6447	The FULL – Cliente plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the license plan parameter in all versions up to, and including, 3.1.12 due to insufficient input sanitization and output escaping as well as missing authorization and capability checks on the related functions. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute whenever an administrative user accesses wp-admin dashboard	7.2	More Details
CVE-2024-37149	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated technician user can upload a malicious PHP script and hijack the plugin loader to execute this malicious script. Upgrade to 10.0.16.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48866	In the Linux kernel, the following vulnerability has been resolved: HID: hid-thrustmaster: fix OOB read in thrustmaster_interrupts Syzbot reported an slab-out-of-bounds Read in thrustmaster_probe() bug. The root case is in missing validation check of actual number of endpoints. Code should not blindly access usb_host_interface::endpoint array, since it may contain less endpoints than code expects. Fix it by adding missing validaion check and print an error if number of endpoints do not match expected number	7.1	More Details
CVE-2024-27238	Race condition in the installer for some Zoom Apps and SDKs for Windows before version 6.0.0 may allow an authenticated user to conduct a privilege escalation via local access.	7.1	More Details
CVE-2024-5679	CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, or kernel memory leak when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	7.1	More Details
CVE-2024-5680	CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	7.1	More Details
CVE-2024-27240	Improper input validation in the installer for some Zoom Apps for Windows may allow an authenticated user to conduct a privilege escalation via local access.	7.1	More Details
CVE-2024-38717	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Booking Ultra Pro allows PHP Local File Inclusion.This issue affects Booking Ultra Pro: from n/a through 1.1.13.	7.1	More Details
CVE-2021-47624	In the Linux kernel, the following vulnerability has been resolved: net/sunrpc: fix reference count leaks in rpc_sysfs_xprt_state_change The refcount leak issues take place in an error handling path. When the 3rd argument buf doesn't match with "offline", "online" or "remove", the function simply returns -EINVAL and forgets to decrease the reference count of a rpc_xprt object and a rpc_xprt_switch object increased by rpc_sysfs_xprt_kobj_get_xprt() and rpc_sysfs_xprt_kobj_get_xprt_switch(), causing reference count leaks of both unused objects. Fix this issue by jumping to the error handling path labelled with out_put when buf matches none of "offline", "online" or "remove".	7.1	More Details
CVE-2022-48820	In the Linux kernel, the following vulnerability has been resolved: phy: stm32: fix a refcount leak in stm32_usbphyc_pll_enable() This error path needs to decrement "usbphyc->n_pll_cons.counter" before returning.	7.1	More Details
CVE-2024-5151	The SULly WordPress plugin before 4.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	7.1	More Details
CVE-2024-32469	Decidim is a participatory democracy framework. The pagination feature used in searches and filters is subject to potential XSS attack through a malformed URL using the GET parameter `per_page`. This vulnerability is fixed in 0.27.6 and 0.28.1.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48855	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline] simple_copy_to_iter+0xf3/0x140 net/core/datagram.c:519 __skb_datagram_iter+0x2d5/0x11b0 net/core/datagram.c:425 skb_copy_datagram_iter+0xdc/0x270 net/core/datagram.c:533 skb_copy_datagram_msg include/linux/skbuff.h:3696 [inline] netlink_recvmsg+0x669/0x1c80 net/netlink/af_netlink.c:1977 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom+0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341 sock_diag_rcv_msg+0x24a/0x620 netlink_rcv_skb+0x40c/0x7e0 net/netlink/af_netlink.c:2494 sock_diag_rcv+0x63/0x80 net/core/sock_diag.c:277 netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline] netlink_unicast+0x1093/0x1360 net/netlink/af_netlink.c:1343 netlink_sendmsg+0x14d9/0x1720 net/netlink/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x594/0x690 net/socket.c:1061 do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011	7.1	More Details
CVE-2024-1937	The Brizy – Page Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_item' function in all versions up to, and including, 2.4.44. This makes it possible for authenticated attackers, with contributor access and above, to modify the content of arbitrary published posts, which includes the ability to insert malicious JavaScript.	7.1	More Details
CVE-2024-37213	Cross-Site Request Forgery (CSRF) vulnerability in Ali2Woo Team Ali2Woo Lite allows Cross-Site Scripting (XSS).This issue affects Ali2Woo Lite: from n/a through 3.3.9.	7.1	More Details
CVE-2024-5287	The wp-affiliate-platform WordPress plugin before 6.5.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in user change them via a CSRF attack	7.1	More Details
CVE-2024-35773	Cross-Site Request Forgery (CSRF) vulnerability in WPJohnny, zerOneIT Comment Reply Email allows Cross-Site Scripting (XSS).This issue affects Comment Reply Email: from n/a through 1.3.	7.1	More Details
CVE-2024-5472	The WP QuickLaTeX WordPress plugin before 3.8.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	7.1	More Details
CVE-2024-5715	The wp-eMember WordPress plugin before 10.6.7 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	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48858	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix a race on command flush flow Fix a refcount use after free warning due to a race on command entry. Such race occurs when one of the commands releases its last refcount and frees its index and entry while another process running command flush flow takes refcount to this command entry. The process which handles commands flush may see this command as needed to be flushed if the other process released its refcount but didn't release the index yet. Fix it by adding the needed spin lock. It fixes the following warning trace: refcount_t: addition on 0; use-after-free. WARNING: CPU: 11 PID: 540311 at lib/refcount.c:25 refcount_warn_saturate+0x80/0xe0 ... RIP: 0010:refcount_warn_saturate+0x80/0xe0 ... Call Trace: <TASK> mlx5_cmd_trigger_completions+0x293/0x340 [mlx5_core] mlx5_cmd_flush+0x3a/0xf0 [mlx5_core] enter_error_state+0x44/0x80 [mlx5_core] mlx5_fw_fatal_reporter_err_work+0x37/0xe0 [mlx5_core] process_one_work+0x1be/0x390 worker_thread+0x4d/0x3d0 ? rescuer_thread+0x350/0x350 kthread+0x141/0x160 ? set_kthread_struct+0x40/0x40 ret_from_fork+0x1f/0x30 </TASK>	7.0	More Details
CVE-2022-48790	In the Linux kernel, the following vulnerability has been resolved: nvme: fix a possible use-after-free in controller reset during load Unlike .queue_rq, in .submit_async_event drivers may not check the ctrl readiness for AER submission. This may lead to a use-after-free condition that was observed with nvme-tcp. The race condition may happen in the following scenario: 1. driver executes its reset_ctrl_work 2. -> nvme_stop_ctrl - flushes ctrl async_event_work 3. ctrl sends AEN which is received by the host, which in turn schedules AEN handling 4. teardown admin queue (which releases the queue socket) 5. AEN processed, submits another AER, calling the driver to submit 6. driver attempts to send the cmd ==> use-after-free In order to fix that, add ctrl state check to validate the ctrl is actually able to accept the AER submission. This addresses the above race in controller resets because the driver during teardown should: 1. change ctrl state to RESETTING 2. flush async_event_work (as well as other async work elements) So after 1,2, any other AER command will find the ctrl state to be RESETTING and bail out without submitting the AER.	7.0	More Details
CVE-2024-6655	A flaw was found in the GTK library. Under certain conditions, it is possible for a library to be injected into a GTK application from the current working directory.	7.0	More Details
CVE-2024-39492	In the Linux kernel, the following vulnerability has been resolved: mailbox: mtk-cmdq: Fix pm_runtime_get_sync() warning in mbox shutdown The return value of pm_runtime_get_sync() in cmdq_mbox_shutdown() will return 1 when pm runtime state is active, and we don't want to get the warning message in this case. So we change the return value < 0 for WARN_ON().	7.0	More Details
CVE-2024-3710	The Image Photo Gallery Final Tiles Grid WordPress plugin before 3.6.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin	6.8	More Details
CVE-2024-22387	External Control of Critical State Data (CWE-642) in the Controller 6000 and Controller 7000 diagnostic web interface allows an authenticated user to modify device I/O connections leading to unexpected behavior that in some circumstances could compromise site physical security controls. Gallagher recommend the diagnostic web page is not enabled (default is off) unless advised by Gallagher Technical support. This interface is intended only for diagnostic purposes. This issue affects: Gallagher Controller 6000 and 7000 9.10 prior to vCR9.10.240520a (distributed in 9.10.1268(MR1)), 9.00 prior to vCR9.00.240521a (distributed in 9.00.1990(MR3)), 8.90 prior to vCR8.90.240520a (distributed in 8.90.1947 (MR4)), 8.80 prior to vCR8.80.240520a (distributed in 8.80.1726 (MR5)), 8.70 prior to vCR8.70.240520a (distributed in 8.70.2824 (MR7)), all versions of 8.60 and prior.	6.8	More Details
CVE-2024-39826	Path traversal in Team Chat for some Zoom Workplace Apps and SDKs for Windows may allow an authenticated user to conduct information disclosure via network access.	6.8	More Details
CVE-2024-40412	Tenda AX12 v1.0 v22.03.01.46 contains a stack overflow in the deviceList parameter of the sub_42E410 function.	6.8	More Details
CVE-2024-37016	Mengshen Wireless Door Alarm M70 2024-05-24 allows Authentication Bypass via a Capture-Replay approach.	6.8	More Details
CVE-2024-5284	The wp-affiliate-platform WordPress plugin before 6.5.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	6.8	More Details
CVE-2024-5077	The wp-eMember WordPress plugin before 10.6.6 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5744	The wp-eMember WordPress plugin before 10.6.7 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	6.8	More Details
CVE-2024-4977	The Index WP MySQL For Speed WordPress plugin before 1.4.18 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	6.8	More Details
CVE-2024-25076	An issue was discovered on Renesas SmartBond DA14691, DA14695, DA14697, and DA14699 devices. The bootrom function responsible for validating the Flash Product Header directly uses a user-controllable size value (Length of Flash Config Section) to control a read from the QSPI device into a fixed sized buffer, resulting in a buffer overflow and execution of arbitrary code.	6.8	More Details
CVE-2024-3632	The Smart Image Gallery WordPress plugin before 1.0.19 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.8	More Details
CVE-2024-38301	Dell Alienware Command Center, version 5.7.3.0 and prior, contains an improper access control vulnerability. A low privileged attacker could potentially exploit this vulnerability, leading to denial of service on the local system and information disclosure.	6.7	More Details
CVE-2024-38433	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution.	6.7	More Details
CVE-2024-39819	Improper privilege management in the installer for some Zoom Workplace Apps and SDKs for Windows may allow an authenticated user to conduct a privilege escalation via local access.	6.7	More Details
CVE-2024-20456	A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Cisco Secure Boot functionality and load unverified software on an affected device. To exploit this successfully, the attacker must have root-system privileges on the affected device. This vulnerability is due to an error in the software build process. An attacker could exploit this vulnerability by manipulating the system’s configuration options to bypass some of the integrity checks that are performed during the booting process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass of the requirement to run Cisco signed images or alter the security properties of the running system.	6.7	More Details
CVE-2024-39820	Uncontrolled search path element in the installer for Zoom Workplace Desktop App for macOS before version 6.0.10 may allow an authenticated user to conduct a denial of service via local access.	6.6	More Details
CVE-2024-39512	An Improper Physical Access Control vulnerability in the console port control of Juniper Networks Junos OS Evolved allows an attacker with physical access to the device to get access to a user account. When the console cable is disconnected, the logged in user is not logged out. This allows a malicious attacker with physical access to the console to resume a previous session and possibly gain administrative privileges. This issue affects Junos OS Evolved: * from 23.2R2-EVO before 23.2R2-S1-EVO, * from 23.4R1-EVO before 23.4R2-EVO.	6.6	More Details
CVE-2024-39821	Race condition in the installer for Zoom Workplace App for Windows and Zoom Rooms App for Windows may allow an authenticated user to conduct a denial of service via local access.	6.6	More Details
CVE-2024-5028	The CM WordPress Search And Replace Plugin WordPress plugin before 1.3.9 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	6.5	More Details
CVE-2024-39736	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 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. IBM X-Force ID: 296003.	6.5	More Details
CVE-2024-3963	The Giveaways and Contests by RafflePress WordPress plugin before 1.12.14 does not sanitise and escape some parameters, which could allow users with a role as low as editor to perform Cross-Site Scripting attacks	6.5	More Details
CVE-2024-38700	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in realmag777 WPCS allows Code Injection.This issue affects WPCS: from n/a through 1.2.0.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37202	Missing Authorization vulnerability in BinaryCarpenter Ultimate Custom Add To Cart Button (Ajax) For WooCommerce by Binary Carpenter allows Cross-Site Scripting (XSS).This issue affects Ultimate Custom Add To Cart Button (Ajax) For WooCommerce by Binary Carpenter: from n/a through 1.222.16.	6.5	More Details
CVE-2024-40547	PublicCMS v4.0.202302.e was discovered to contain an arbitrary file content replacement vulnerability via the component /admin/cmsTemplate/replace.	6.5	More Details
CVE-2023-41916	In Apache Linkis =1.4.0, due to the lack of effective filtering of parameters, an attacker configuring malicious Mysql JDBC parameters in the DataSource Manager Module will trigger arbitrary file reading. Therefore, the parameters in the Mysql JDBC URL should be blacklisted. This attack requires the attacker to obtain an authorized account from Linkis before it can be carried out. Versions of Apache Linkis = 1.4.0 will be affected. We recommend users upgrade the version of Linkis to version 1.5.0.	6.5	More Details
CVE-2024-38704	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in DynamicWebLab WordPress Team Manager allows PHP Local File Inclusion.This issue affects WordPress Team Manager: from n/a through 2.1.12.	6.5	More Details
CVE-2024-31947	StoneFly Storage Concentrator (SC and SCVM) before 8.0.4.26 allows Directory Traversal by authenticated users. Using a crafted path parameter with the Online Help facility can expose sensitive system information.	6.5	More Details
CVE-2023-39329	A flaw was found in OpenJPEG. A resource exhaustion can occur in the opj_t1_decode_cblks function in tcd.c through a crafted image file, causing a denial of service.	6.5	More Details
CVE-2024-38716	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Blue Plugins Events Calendar for Google allows PHP Local File Inclusion.This issue affects Events Calendar for Google: from n/a through 2.1.0.	6.5	More Details
CVE-2024-39909	KubeClarity is a tool for detection and management of Software Bill Of Materials (SBOM) and vulnerabilities of container images and filesystems. A time/boolean SQL Injection is present in the following resource `/api/applicationResources` via the following parameter `packageID`. As it can be seen in backend/pkg/database/id_view.go, while building the SQL Query the `fmt.Sprintf` function is used to build the query string without the input having first been subjected to any validation. This vulnerability is fixed in 2.23.1.	6.5	More Details
CVE-2024-38715	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ExS ExS Widgets allows PHP Local File Inclusion.This issue affects ExS Widgets: from n/a through 0.3.1.	6.5	More Details
CVE-2024-38706	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in HasThemes HT Mega allows Path Traversal.This issue affects HT Mega: from n/a through 2.5.7.	6.5	More Details
CVE-2024-5500	Inappropriate implementation in Sign-In in Google Chrome prior to 1.3.36.351 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-6325	The v6.40 release of Rockwell Automation FactoryTalk® Policy Manager CVE-2021-22681 https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1550.html and CVE-2022-1161 https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1585.html by implementing CIP security and did not update to the versions of the software CVE-2022-1161 https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1585.html and CVE-2022-1161. https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1585.html	6.5	More Details
CVE-2024-39517	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Layer 2 Address Learning Daemon (l2ald) on Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause Denial of Service (DoS). In an EVPN/VXLAN scenario, when a high amount specific Layer 2 packets are processed by the device, it can cause the Routing Protocol Daemon (rpd) to utilize all CPU resources which causes the device to hang. A manual restart of the rpd is required to restore services. This issue affects both IPv4 and IPv6 implementations. This issue affects Junos OS: All versions earlier than 21.4R3-S7; 22.1 versions earlier than 22.1R3-S5; 22.2 versions earlier than 22.2R3-S3; 22.3 versions earlier than 22.3R3-S3; 22.4 versions earlier than 22.4R3-S2; 23.2 versions earlier than 23.2R2; 23.4 versions earlier than 23.4R1-S1. Junos OS Evolved: All versions earlier than 21.4R3-S7-EVO; 22.1-EVO versions earlier than 22.1R3-S5-EVO; 22.2-EVO versions earlier than 22.2R3-S3-EVO; 22.3-EVO versions earlier than 22.3R3-S3-EVO; 22.4-EVO versions earlier than 22.4R3-S2-EVO; 23.2-EVO versions earlier than 23.2R2-EVO; 23.4-EVO versions earlier than 23.4R1-S1-EVO, 23.4R2-EVO.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39535	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX 7000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). When a device has a Layer 3 or an IRB interface configured in a VPLS instance and specific traffic is received, the evo-pfemand processes crashes which causes a service outage for the respective FPC until the system is recovered manually. This issue only affects Junos OS Evolved 22.4R2-S1 and 22.4R2-S2 releases and is fixed in 22.4R3. No other releases are affected.	6.5	More Details
CVE-2024-39537	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved on ACX 7000 Series allows an unauthenticated, network-based attacker to cause a limited information disclosure and availability impact to the device. Due to a wrong initialization, specific processes which should only be able to communicate internally within the device can be reached over the network via open ports. This issue affects Junos OS Evolved on ACX 7000 Series: * All versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-S3-EVO, * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO, * 23.4-EVO versions before 23.4R1-S1-EVO, 23.4R2-EVO.	6.5	More Details
CVE-2024-39538	A Buffer Copy without Checking Size of Input vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS).When multicast traffic with a specific, valid (S,G) is received, evo-pfemand crashes which leads to an outage of the affected FPC until it is manually recovered. This issue affects Junos OS Evolved on ACX7000 Series: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-S3-EVO, * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO, * 23.4-EVO versions before 23.4R1-S2-EVO, 23.4R2-EVO.	6.5	More Details
CVE-2024-39036	SeaCMS v12.9 is vulnerable to Arbitrary File Read via admin_safe.php.	6.5	More Details
CVE-2024-39541	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). When conflicting information (IP or ISO addresses) about a node is added to the Traffic Engineering (TE) database and then a subsequent operation attempts to process these, rpd will crash and restart. This issue affects: Junos OS: * 22.4 versions before 22.4R3-S1, * 23.2 versions before 23.2R2, * 23.4 versions before 23.4R1-S1, 23.4R2, This issue does not affect Junos OS versions earlier than 22.4R1. Junos OS Evolved: * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO, * 23.4-EVO versions before 23.4R1-S1-EVO, 23.4R2-EVO, This issue does not affect Junos OS Evolved versions earlier than before 22.4R1.	6.5	More Details
CVE-2024-40503	An issue in Tenda AX12 v.16.03.49.18_cn+ allows a remote attacker to cause a denial of service via the Routing functionality and ICMP packet handling.	6.5	More Details
CVE-2024-5815	A Cross-Site Request Forgery vulnerability in GitHub Enterprise Server allowed write operations on a victim-owned repository by exploiting incorrect request types. A mitigating factor is that the attacker would have to be a trusted GitHub Enterprise Server user, and the victim would have to visit a tag in the attacker's fork of their own repository. vulnerability affected all versions of GitHub Enterprise Server prior 3.14 and was fixed in version 3.13.1, 3.12.6, 3.11.12, 3.10.14, and 3.9.17. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2024-5817	An Incorrect Authorization vulnerability was identified in GitHub Enterprise Server that allowed read access to issue content via GitHub Projects. This was only exploitable in internal repositories and required the attacker to have access to the corresponding project board. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.13.1, 3.12.6, 3.11.12, 3.10.14, and 3.9.17. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2024-39560	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a logically adjacent downstream RSVP neighbor to cause kernel memory exhaustion, leading to a kernel crash, resulting in a Denial of Service (DoS). The kernel memory leak and eventual crash will be seen when the downstream RSVP neighbor has a persistent error which will not be corrected. System kernel memory can be monitored through the use of the 'show system kernel memory' command as shown below: user@router> show system kernel memory Real memory total/reserved: 4130268/ 133344 Kbytes kmem map free: 18014398509110220 Kbytes This issue affects: Junos OS: * All versions before 20.4R3-S9, * All versions of 21.2, * from 21.4 before 21.4R3-S5, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2; Junos OS Evolved: * All versions before 21.4R3-S5-EVO, * from 22.1-EVO before 22.1R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S2-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39558	An Unchecked Return Value vulnerability in the Routing Protocol Daemon (rpd) on Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows a logically adjacent, unauthenticated attacker sending a specific PIM packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS), when PIM is configured with Multicast-only Fast Reroute (MoFRR). Continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. This issue is observed on Junos and Junos Evolved platforms where PIM is configured along with MoFRR. MoFRR tries to select the active path, but due to an internal timing issue, rpd is unable to select the forwarding next-hop towards the source, resulting in an rpd crash. This issue affects: Junos OS: * All versions before 20.4R3-S10, * from 21.2 before 21.2R3-S7, * from 21.4 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3, * from 22.4 before 22.4R2; Junos OS Evolved: * All versions before 20.4R3-S10 -EVO, * All versions of 21.2-EVO, * from 21.4-EVO before 21.4R3-S9-EVO, * from 22.1-EVO before 22.1R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-EVO, * from 22.4-EVO before 22.4R2-EVO.	6.5	More Details
CVE-2024-39557	An Uncontrolled Resource Consumption vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a memory leak, eventually exhausting all system memory, leading to a system crash and Denial of Service (DoS). Certain MAC table updates cause a small amount of memory to leak. Once memory utilization reaches its limit, the issue will result in a system crash and restart. To identify the issue, execute the CLI command: user@device> show platform application-info allocations app l2ald-agent EVL Object Allocation Statistics: Node Application Context Name Live Allocs Fails Guids re0 l2ald-agent net::juniper::rtnh::L2Rtinfo 1069096 1069302 0 1069302 re0 l2ald-agent net::juniper::rtnh::NHOpaqueTlv 114 195 0 195 This issue affects Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	6.5	More Details
CVE-2024-39543	A Buffer Copy without Checking Size of Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows an unauthenticated, adjacent attacker to send specific RPKI-RTR packets resulting in a crash, creating a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects Junos OS: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S8, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R2. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * from 21.4 before 21.4R3-S8-EVO, * from 22.2 before 22.2R3-S4-EVO, * from 22.3 before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-S2-EVO, * from 23.2 before 23.2R2-S1-EVO, * from 23.4 before 23.4R2-EVO.	6.5	More Details
CVE-2024-39550	A Missing Release of Memory after Effective Lifetime vulnerability in the rtlogd process of Juniper Networks Junos OS on MX Series with SPC3 allows an unauthenticated, adjacent attacker to trigger internal events cause (which can be done by repeated port flaps) to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Memory can only be recovered by manually restarting rtlogd process. The memory usage can be monitored using the below command. user@host> show system processes extensive l match rtlog This issue affects Junos OS on MX Series with SPC3 line card: * from 21.2R3 before 21.2R3-S8, * from 21.4R2 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3-S1, * from 23.2 before 23.2R2, * from 23.4 before 23.4R2.	6.5	More Details
CVE-2024-39519	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). On all ACX 7000 Series platforms running Junos OS Evolved, and configured with IRBs, if a Customer Edge device (CE) device is dual homed to two Provider Edge devices (PE) a traffic loop will occur when the CE sends multicast packets. This issue can be triggered by IPv4 and IPv6 traffic. This issue affects Junos OS Evolved: All versions from 22.2R1-EVO and later versions before 22.4R2-EVO, This issue does not affect Junos OS Evolved versions before 22.1R1-EVO.	6.5	More Details
CVE-2024-39553	An Exposure of Resource to Wrong Sphere vulnerability in the sampling service of Juniper Networks Junos OS Evolved allows an unauthenticated network-based attacker to send arbitrary data to the device, which leads msvcsd process to crash with limited availability impacting Denial of Service (DoS) and allows unauthorized network access to the device, potentially impacting system integrity. This issue only happens when inline jflow is configured. This does not impact any forwarding traffic. The impacted services MSVCS-DB app crashes momentarily and recovers by itself. This issue affects Juniper Networks Junos OS Evolved: * 21.4 versions earlier than 21.4R3-S7-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO; * 22.3 versions earlier than 22.3R3-S2-EVO; * 22.4 versions earlier than 22.4R3-EVO; * 23.2 versions earlier than 23.2R1-S2-EVO, 23.2R2-EVO.	6.5	More Details
CVE-2024-21169	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Partners). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data as well as unauthorized read access to a subset of Oracle Marketing accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21168	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are Prior to 9.2.8.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2024-40417	A vulnerability was found in Tenda AX1806 1.0.0.1. Affected by this issue is the function formSetRebootTimer of the file /goform/SetIpMacBind. The manipulation of the argument list leads to stack-based buffer overflow.	6.5	More Details
CVE-2024-2884	Out of bounds read in V8 in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-21177	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-21171	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-39514	An Improper Check or Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). An attacker can send specific traffic to the device, which causes the rpd to crash and restart. Continued receipt of this traffic will result in a sustained DoS condition. This issue only affects devices with an EVPN-VPWS instance with IGMP-snooping enabled. This issue affects Junos OS: * All versions before 20.4R3-S10, * from 21.4 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2; Junos OS Evolved: * All versions before 20.4R3-S10-EVO, * from 21.4-EVO before 21.4R3-S6-EVO, * from 22.1-EVO before 22.1R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S2-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	6.5	More Details
CVE-2024-39317	Wagtail is an open source content management system built on Django. A bug in Wagtail's `parse_query_string` would result in it taking a long time to process suitably crafted inputs. When used to parse sufficiently long strings of characters without a space, `parse_query_string` would take an unexpectedly large amount of time to process, resulting in a denial of service. In an initial Wagtail installation, the vulnerability can be exploited by any Wagtail admin user. It cannot be exploited by end users. If your Wagtail site has a custom search implementation which uses `parse_query_string`, it may be exploitable by other users (e.g. unauthenticated users). Patched versions have been released as Wagtail 5.2.6, 6.0.6 and 6.1.3.	6.5	More Details
CVE-2023-7011	Inappropriate implementation in Picture in Picture in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2020-36765	Insufficient policy enforcement in Navigation in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-6777	Use after free in Navigation in Google Chrome prior to 126.0.6478.182 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	6.5	More Details
CVE-2024-21158	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39916	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. There is a security issue with the NFS configuration in /etc/exports generated by the installer that allows an attacker to modify files outside the export in the default installation. The exports have the no_subtree_check option. The no_subtree_check option means that if a client performs a file operation, the server will only check if the requested file is on the correct filesystem, not if it is in the correct directory. This enables modifying files in /images, accessing other files on the same filesystem, and accessing files on other filesystems. This vulnerability is fixed in 1.5.10.30.	6.4	More Details
CVE-2024-39556	A Stack-Based Buffer Overflow vulnerability in Juniper Networks Junos OS and Juniper Networks Junos OS Evolved may allow a local, low-privileged attacker with access to the CLI the ability to load a malicious certificate file, leading to a limited Denial of Service (DoS) or privileged code execution. By exploiting the 'set security certificates' command with a crafted certificate file, a malicious attacker with access to the CLI could cause a crash of the command management daemon (mgd), limited to the local user's command interpreter, or potentially trigger a stack-based buffer overflow. This issue affects: Junos OS: * All versions before 21.4R3-S7, * from 22.1 before 22.1R3-S6, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S1, 23.4R2; Junos OS Evolved: * All versions before 21.4R3-S7-EVO, * from 22.1-EVO before 22.1R3-S6-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-S2-EVO, * from 23.2-EVO before 23.2R2-EVO, * from 23.4-EVO before 23.4R1-S1-EVO, 23.4R2-EVO.	6.4	More Details
CVE-2024-2691	The WP Event Manager – Events Calendar, Registrations, Sell Tickets with WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'events' shortcode in all versions up to, and including, 3.1.43 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-2024-6256	The Feeds for YouTube (YouTube video, channel, and gallery plugin) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'youtube-feed' shortcode in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4866	The UltraAddons – Elementor Addons (Header Footer Builder, Custom Font, Custom CSS,Woo Widget, Menu Builder, Anywhere Elementor Shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6495	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Animated Text widget in all versions up to, and including, 4.10.36 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-2024-5664	The MP3 Audio Player – Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' attribute within the plugin's sonaar_audioplayer shortcode in all versions up to, and including, 5.5 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-2024-4780	The Image Hover Effects – Elementor Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘eihe_link’ parameter in all versions up to, and including, 1.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6485	A security vulnerability has been discovered in bootstrap that could enable Cross-Site Scripting (XSS) attacks. The vulnerability is associated with the data-loading-text attribute within the button plugin. This vulnerability can be exploited by injecting malicious JavaScript code into the attribute, which would then be executed when the button's loading state is triggered.	6.4	More Details
CVE-2024-3587	The Premium Portfolio Features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Grid Portfolios Widget in all versions up to, and including, 2.3.2 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 Number	Description	Base Score	Reference
CVE-2023-52886	In the Linux kernel, the following vulnerability has been resolved: USB: core: Fix race by not overwriting udev->descriptor in hub_port_init() Syzbot reported an out-of-bounds read in sysfs.c:read_descriptors(): BUG: KASAN: slab-out-of-bounds in read_descriptors+0x263/0x280 drivers/usb/core/sysfs.c:883 Read of size 8 at addr ffff88801e78b8c8 by task udevd/5011 CPU: 0 PID: 5011 Comm: udevd Not tainted 6.4.0-rc6-syzkaller-00195-g40f71e7cd3c6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/27/2023 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x150 lib/dump_stack.c:106 print_address_description.constprop.0+0x2c/0x3c0 mm/kasan/report.c:351 print_report mm/kasan/report.c:462 [inline] kasan_report+0x11c/0x130 mm/kasan/report.c:572 read_descriptors+0x263/0x280 drivers/usb/core/sysfs.c:883 ... Allocated by task 758: ... __do_kmalloc_node mm/slab_common.c:966 [inline] __kmalloc+0x5e/0x190 mm/slab_common.c:979 kmalloc include/linux/slab.h:563 [inline] kzalloc include/linux/slab.h:680 [inline] usb_get_configuration+0x1f7/0x5170 drivers/usb/core/config.c:887 usb_enumerate_device drivers/usb/core/hub.c:2407 [inline] usb_new_device+0x12b0/0x19d0 drivers/usb/core/hub.c:2545 As analyzed by Khazhy Kumykov, the cause of this bug is a race between read_descriptors() and hub_port_init(): The first routine uses a field in udev->descriptor, not expecting it to change, while the second overwrites it. Prior to commit 45bf39f8df7f ("USB: core: Don't hold device lock while reading the "descriptors" sysfs file") this race couldn't occur, because the routines were mutually exclusive thanks to the device locking. Removing that locking from read_descriptors() exposed it to the race. The best way to fix the bug is to keep hub_port_init() from changing udev->descriptor once udev has been initialized and registered. Drivers expect the descriptors stored in the kernel to be immutable; we should not undermine this expectation. In fact, this change should have been made long ago. So now hub_port_init() will take an additional argument, specifying a buffer in which to store the device descriptor it reads. (If udev has not yet been initialized, the buffer pointer will be NULL and then hub_port_init() will store the device descriptor in udev as before.) This eliminates the data race responsible for the out-of-bounds read. The changes to hub_port_init() appear more extensive than they really are, because of indentation changes resulting from an attempt to avoid writing to other parts of the usb_device structure after it has been initialized. Similar changes should be made to the code that reads the BOS descriptor, but that can be handled in a separate patch later on. This patch is sufficient to fix the bug found by syzbot.	6.4	More Details
CVE-2024-39728	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 295967.	6.4	More Details
CVE-2024-6531	A vulnerability has been identified in Bootstrap that exposes users to Cross-Site Scripting (XSS) attacks. The issue is present in the carousel component, where the data-slide and data-slide-to attributes can be exploited through the href attribute of an <a> tag due to inadequate sanitization. This vulnerability could potentially enable attackers to execute arbitrary JavaScript within the victim's browser.	6.4	More Details
CVE-2024-6588	The PowerPress Podcasting plugin by Blubrry plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘media_url’ parameter in all versions up to, and including, 11.9.10 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.	6.4	More Details
CVE-2024-6484	A vulnerability has been identified in Bootstrap that exposes users to Cross-Site Scripting (XSS) attacks. The issue is present in the carousel component, where the data-slide and data-slide-to attributes can be exploited through the href attribute of an <a> tag due to inadequate sanitization. This vulnerability could potentially enable attackers to execute arbitrary JavaScript within the victim's browser.	6.4	More Details
CVE-2024-21170	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/Python). Supported versions that are affected are 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	6.3	More Details
CVE-2024-40328	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/memberOnline_deal.php?mudi=del&dataType=&dataID=6	6.3	More Details
CVE-2022-29946	NATS.io NATS Server before 2.8.2 and Streaming Server before 0.24.6 could allow a remote attacker to bypass security restrictions, caused by the failure to enforce negative user permissions in one scenario. By using a queue subscription on the wildcard, an attacker could exploit this vulnerability to allow denied subjects.	6.3	More Details
CVE-2024-6736	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been rated as critical. This issue affects some unknown processing of the file view_employee.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271457 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6645	A vulnerability was found in WuKongOpenSource Wukong_nocode up to 20230807. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file ExpressionUtil.java of the component AviatorScript Handler. The manipulation leads to deserialization. The attack can be launched 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. The associated identifier of this vulnerability is VDB-271051.	6.3	More Details
CVE-2024-6681	A vulnerability, which was classified as critical, has been found in witmy my-springsecurity-plus up to 2024-07-04. Affected by this issue is some unknown functionality of the file /api/dept. 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. VDB-271154 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6735	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file setgeneral.php. The manipulation of the argument sitename/email/mobile/sms/currency leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271456.	6.3	More Details
CVE-2024-6734	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file templateadd.php. The manipulation of the argument title/msg leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-271455.	6.3	More Details
CVE-2024-6733	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file templateedit.php. The manipulation of the argument id/title/msg leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-271454 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6732	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. This vulnerability affects unknown code of the file /sscdms/classes/Users.php?f=save. 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-2024-6644	A vulnerability was found in zmops ArgusDBM up to 0.1.0. It has been classified as critical. Affected is the function getDefaultClassLoader of the file CalculateAlarm.java of the component AviatorScript Handler. The manipulation leads to deserialization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-271050 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6652	A vulnerability was found in itsourcecode Gym Management System 1.0. It has been classified as critical. This affects an unknown part of the file manage_member.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. The associated identifier of this vulnerability is VDB-271059.	6.3	More Details
CVE-2024-6728	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file typeedit.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. The identifier VDB-271401 was assigned to this vulnerability.	6.3	More Details
CVE-2020-25836	Exposure of Sensitive Information to an Unauthorized Access vulnerability in OpenText NetIQ Directory and Resource Administrator. This issue affects NetIQ Directory and Resource Administrator versions prior to 10.0.2 and prior to 9.2.1 Patch 10.	6.3	More Details
CVE-2024-23317	External Control of File Name or Path (CWE-73) in the Controller 6000 and Controller 7000 allows an attacker with local access to the Controller to perform arbitrary code execution. This issue affects: 9.10 prior to vCR9.10.240520a (distributed in 9.10.1268(MR1)), 9.00 prior to vCR9.00.240521a (distributed in 9.00.1990(MR3)), 8.90 prior to vCR8.90.240520a (distributed in 8.90.1947 (MR4)), 8.80 prior to vCR8.80.240520a (distributed in 8.80.1726 (MR5)), 8.70 prior to vCR8.70.240520a (distributed in 8.70.2824 (MR7)), all versions of 8.60 and prior.	6.3	More Details
CVE-2024-6676	A vulnerability has been found in witmy my-springsecurity-plus up to 2024-07-03 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /api/user. 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. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-271111.	6.3	More Details
CVE-2024-6731	A vulnerability classified as critical has been found in SourceCodester Student Study Center Desk Management System 1.0. This affects an unknown part of the file /Master.php?f=save_student. 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 Number	Description	Base Score	Reference
CVE-2024-3175	Insufficient data validation in Extensions in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Low)	6.3	More Details
CVE-2024-6730	A vulnerability was found in Nanjing Xingyuantu Technology SparkShop up to 1.1.6. It has been rated as critical. This issue affects some unknown processing of the file /api/Common/uploadFile. The manipulation of the argument file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-271403.	6.3	More Details
CVE-2024-6729	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /control/add_act.php. The manipulation of the argument aname 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-2016-15039	A vulnerability classified as critical was found in mhuertos phpLDAPadmin up to 665dbc2690ebeb5392d38f1fece0a654225a0b38. Affected by this vulnerability is the function makeHttpRequest of the file htdocs/js/ajax_functions.js. The manipulation leads to http request smuggling. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named dd6e9583a2eb2ca085583765e8a63df5904cb036. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-270523.	6.3	More Details
CVE-2024-6680	A vulnerability classified as critical was found in witmy my-springsecurity-plus up to 2024-07-04. Affected by this vulnerability is an unknown functionality of the file /api/dept/build. 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. The identifier VDB-271153 was assigned to this vulnerability.	6.3	More Details
CVE-2024-39532	An Insertion of Sensitive Information into Log File vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, authenticated attacker with high privileges to access sensitive information. When another user performs a specific operation, sensitive information is stored as plain text in a specific log file, so that a high-privileged attacker has access to this information. This issue affects: Junos OS: * All versions before 22.1R2-S2, * 22.1R3 and later versions, * 22.2 versions before 22.2R2-S1, 22.2R3, * 22.3 versions before 22.3R1-S2, 22.3R2; Junos OS Evolved: * All versions before before 22.1R3-EVO, * 22.2-EVO versions before 22.2R2-S1-EVO, 22.2R3-EVO, * 22.3-EVO versions before 22.3R1-S1-EVO, 22.3R2-EVO.	6.3	More Details
CVE-2024-6679	A vulnerability classified as critical has been found in witmy my-springsecurity-plus up to 2024-07-04. Affected is an unknown function of the file /api/role. The manipulation of the argument params.dataScope 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 identifier of this vulnerability is VDB-271152.	6.3	More Details
CVE-2024-39490	In the Linux kernel, the following vulnerability has been resolved: ipv6: sr: fix missing sk_buff release in seg6_input_core The seg6_input() function is responsible for adding the SRH into a packet, delegating the operation to the seg6_input_core(). This function uses the skb_cow_head() to ensure that there is sufficient headroom in the sk_buff for accommodating the link-layer header. In the event that the skb_cow_header() function fails, the seg6_input_core() catches the error but it does not release the sk_buff, which will result in a memory leak. This issue was introduced in commit af3b5158b89d ("ipv6: sr: fix BUG due to headroom too small after SRH push") and persists even after commit 7a3f5b0de364 ("netfilter: add netfilter hooks to SRv6 data plane"), where the entire seg6_input() code was refactored to deal with netfilter hooks. The proposed patch addresses the identified memory leak by requiring the seg6_input_core() function to release the sk_buff in the event that skb_cow_head() fails.	6.2	More Details
CVE-2024-38493	A reflected cross-site scripting (XSS) vulnerability exists in the PAM UI web interface. A remote attacker able to convince a PAM user to click on a specially crafted link to the PAM UI web interface could potentially execute arbitrary client-side code in the context of PAM UI.	6.1	More Details
CVE-2024-21178	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21188	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: Chatbot). Supported versions that are affected are 6.0.0.0.0 and 6.1.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Revenue Management and Billing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Revenue Management and Billing accessible data as well as unauthorized read access to a subset of Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-3779	Denial of service vulnerability present shortly after product installation or upgrade, potentially allowed an attacker to render ESET's security product inoperable, provided non-default preconditions were met.	6.1	More Details
CVE-2024-6740	Openfind's Mail2000 does not properly validate email atachments, allowing unauthenticated remote attackers to inject JavaScript code within the attachment and perform Stored Cross-site scripting attacks.	6.1	More Details
CVE-2024-5283	The wp-affiliate-platform WordPress plugin before 6.5.1 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-2024-21150	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are Prior to 9.2.8.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-21133	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Servlet). Supported versions that are affected are 12.2.1.4.0 and 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data as well as unauthorized read access to a subset of Oracle Reports Developer accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2024-6289	The WPS Hide Login WordPress plugin before 1.9.16.4 does not prevent redirects to the login page via the auth_redirect WordPress function, allowing an unauthenticated visitor to access the hidden login page.	6.1	More Details
CVE-2024-6076	The wp-cart-for-digital-products WordPress plugin before 8.5.5 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-2024-6074	The wp-cart-for-digital-products WordPress plugin before 8.5.5 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-2024-6073	The wp-cart-for-digital-products WordPress plugin before 8.5.5 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-2024-6072	The wp-cart-for-digital-products WordPress plugin before 8.5.5 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	6.1	More Details
CVE-2024-5282	The wp-affiliate-platform WordPress plugin before 6.5.1 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 Number	Description	Base Score	Reference
CVE-2024-36453	Cross-site scripting vulnerability exists in session_login.cgi of Webmin versions prior to 1.970 and Usermin versions prior to 1.820. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the website using the product. As a result, a webpage may be altered or sensitive information such as a credential may be disclosed.	6.1	More Details
CVE-2024-2870	The socialdriver-framework WordPress plugin before 2024.04.30 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-2024-4269	The SVG Block WordPress plugin before 1.1.20 does not sanitize SVG file contents, which enables users with at least the author role to SVG with malicious JavaScript to conduct Stored XSS attacks.	6.1	More Details
CVE-2024-4272	The Support SVG WordPress plugin before 1.1.0 does not sanitize SVG file contents, which enables users with at least the author role to SVG with malicious JavaScript to conduct Stored XSS attacks.	6.1	More Details
CVE-2024-5079	The wp-eMember WordPress plugin before 10.6.7 does not sanitise and escape some of the fields when members register, which allows unauthenticated users to perform Stored Cross-Site Scripting attacks	6.1	More Details
CVE-2024-5281	The wp-affiliate-platform WordPress plugin before 6.5.1 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-2023-6813	The Login by Auth0 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘wle’ parameter in all versions up to, and including, 4.6.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-40336	idccms v1.35 is vulnerable to Cross Site Scripting (XSS) within the 'Image Advertising Management.'	6.1	More Details
CVE-2024-5913	An improper input validation vulnerability in Palo Alto Networks PAN-OS software enables an attacker with the ability to tamper with the physical file system to elevate privileges.	6.1	More Details
CVE-2024-6035	A Stored Cross-Site Scripting (XSS) vulnerability exists in gaizhenbiao/chuanhuchatgpt version 20240410. This vulnerability allows an attacker to inject malicious JavaScript code into the chat history file. When a victim uploads this file, the malicious script is executed in the victim's browser. This can lead to user data theft, session hijacking, malware distribution, and phishing attacks.	6.1	More Details
CVE-2024-5626	The Inline Related Posts WordPress plugin before 3.7.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2024-5442	The Photo Gallery, Sliders, Proofing and WordPress plugin before 3.59.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	5.9	More Details
CVE-2024-5033	The SULly WordPress plugin before 4.3.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	5.9	More Details
CVE-2024-4752	The EventON WordPress plugin before 2.2.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.9	More Details
CVE-2024-5075	The wp-eMember WordPress plugin before 10.6.6 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	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39554	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to inject incremental routing updates when BGP multipath is enabled, causing rpd to crash and restart, resulting in a Denial of Service (DoS). Since this is a timing issue (race condition), the successful exploitation of this vulnerability is outside the attacker's control. However, continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. On all Junos OS and Junos OS Evolved platforms with BGP multipath enabled, a specific multipath calculation removes the original next hop from the multipath lead routes nexthop-set. When this change happens, multipath relies on certain internal timing to record the update. Under certain circumstance and with specific timing, this could result in an rpd crash. This issue only affects systems with BGP multipath enabled. This issue affects: Junos OS: * All versions of 21.1 * from 21.2 before 21.2R3-S7, * from 21.4 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2. Junos OS Evolved: * All versions of 21.1-EVO, * All versions of 21.2-EVO, * from 21.4-EVO before 21.4R3-S6-EVO, * from 22.1-EVO before 22.1R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S2-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO. Versions of Junos OS before 21.1R1 are unaffected by this vulnerability. Versions of Junos OS Evolved before 21.1R1-EVO are unaffected by this vulnerability.	5.9	More Details
CVE-2024-39559	An Improper Check for Unusual or Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS Evolved may allow a network-based unauthenticated attacker to crash the device (vmcore) by sending a specific TCP packet over an established TCP session with MD5 authentication enabled, destined to an accessible port on the device, resulting in a Denial of Service (DoS). The receipt of this packet must occur within a specific timing window outside the attacker's control (i.e., race condition). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects dual RE systems with Nonstop Active Routing (NSR) enabled. Exploitation can only occur over TCP sessions with MD5 authentication enabled (e.g., BGP with MD5 authentication). This issue affects Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * from 21.4-EVO before 21.4R3-S6-EVO, * from 22.1-EVO before 22.1R3-S4-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R2-S2-EVO, 22.4R3-EVO.	5.9	More Details
CVE-2024-21166	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H).	5.9	More Details
CVE-2024-3964	The Product Enquiry for WooCommerce WordPress plugin before 3.1.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.9	More Details
CVE-2024-3753	The Hostel WordPress plugin before 1.1.5.3 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	5.9	More Details
CVE-2024-39731	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 295970.	5.9	More Details
CVE-2024-39561	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX4600 and SRX5000 Series allows an attacker to send TCP packets with SYN/FIN or SYN/RST flags, bypassing the expected blocking of these packets. A TCP packet with SYN/FIN or SYN/RST should be dropped in flowd. However, when no-syn-check and Express Path are enabled, these TCP packets are unexpectedly transferred to the downstream network. This issue affects Junos OS on SRX4600 and SRX5000 Series: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S7, * from 22.1 before 22.1R3-S6, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S1, 23.4R2.	5.8	More Details
CVE-2024-39533	An Unimplemented or Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an unauthenticated, network-based attacker to cause a minor integrity impact to downstream networks.If one or more of the following match conditions ip-source-address ip-destination-address arp-type which are not supported for this type of filter, are used in an ethernet switching filter, and then this filter is applied as an output filter, the configuration can be committed but the filter will not be in effect. This issue affects Junos OS on QFX5000 Series and EX4600 Series: * All version before 21.2R3-S7, * 21.4 versions before 21.4R3-S6, * 22.1 versions before 22.1R3-S5, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S2, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2. Please note that the implemented fix ensures these unsupported match conditions cannot be committed anymore.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5566	An improper privilege management vulnerability allowed users to migrate private repositories without having appropriate scopes defined on the related Personal Access Token. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in version 3.13.1, 3.12.6, 3.11.12, 3.10.14, and 3.9.17.	5.8	More Details
CVE-2024-21126	Vulnerability in the Oracle Database Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 19.3-19.23 and 21.3-21.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via DNS to compromise Oracle Database Portable Clusterware. While the vulnerability is in Oracle Database Portable Clusterware, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Portable Clusterware. CVSS 3.1 Base Score 5.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L).	5.8	More Details
CVE-2024-40627	Fastapi OPA is an opensource fastapi middleware which includes auth flow. HTTP `OPTIONS` requests are always allowed by `OpaMiddleware`, even when they lack authentication, and are passed through directly to the application. `OpaMiddleware` allows all HTTP `OPTIONS` requests without evaluating it against any policy. If an application provides different responses to HTTP `OPTIONS` requests based on an entity existing (such as to indicate whether an entity is writable on a system level), an unauthenticated attacker could discover which entities exist within an application. This issue has been addressed in release version 2.0.1. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.8	More Details
CVE-2024-6741	Openfind's Mail2000 has a vulnerability that allows the HttpOnly flag to be bypassed. Unauthenticated remote attackers can exploit this vulnerability using specific JavaScript code to obtain the session cookie with the HttpOnly flag enabled.	5.8	More Details
CVE-2023-32467	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some UEFI code, leading to arbitrary code execution or escalation of privilege.	5.7	More Details
CVE-2024-39528	A Use After Free vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an authenticated, network-based attacker to cause a Denial of Service (DoS).On all Junos OS and Junos Evolved platforms, if a routing-instance deactivation is triggered, and at the same time a specific SNMP request is received, a segmentation fault occurs which causes rpd to crash and restart. This issue affects: Junos OS: * All versions before 21.2R3-S8, * 21.4 versions before 21.4R3-S5, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S2, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S5-EVO, * 22.2-EVO versions before 22.2R3-S3-EVO, * 22.3-EVO versions before 22.3R3-S2-EVO, * 22.4-EVO versions before 22.4R3-EVO, * 23.2-EVO versions before 23.2R2-EVO.	5.7	More Details
CVE-2024-6540	Improper filtering of fields when using the export function in the ticket overview of the external interface in OTRS could allow an authorized user to download a list of tickets containing information about tickets of other customers. The problem only occurs if the TicketSearchLegacyEngine has been disabled by the administrator. This issue affects OTRS: 8.0.X, 2023.X, from 2024.X through 2024.4.x	5.7	More Details
CVE-2023-32472	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40957	In the Linux kernel, the following vulnerability has been resolved: seg6: fix parameter passing when calling NF_HOOK() in End.DX4 and End.DX6 behaviors input_action_end_dx4() and input_action_end_dx6() are called NF_HOOK() for PREROUTING hook, in PREROUTING hook, we should passing a valid indev, and a NULL outdev to NF_HOOK(), otherwise may trigger a NULL pointer dereference, as below: [74830.647293] BUG: kernel NULL pointer dereference, address: 0000000000000090 [74830.655633] #PF: supervisor read access in kernel mode [74830.657888] #PF: error_code(0x0000) - not-present page [74830.659500] PGD 0 P4D 0 [74830.660450] Oops: 0000 [#1] PREEMPT SMP PTI ... [74830.664953] Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 [74830.666569] RIP: 0010:rpfilter_mt+0x44/0x15e [ipt_rpfilter] ... [74830.689725] Call Trace: [74830.690402] <IRQ> [74830.690953] ? show_trace_log_lvl+0x1c4/0x2df [74830.692020] ? show_trace_log_lvl+0x1c4/0x2df [74830.693095] ? ipt_do_table+0x286/0x710 [ip_tables] [74830.694275] ? __die_body.cold+0x8/0xd [74830.695205] ? page_fault_oops+0xac/0x140 [74830.696244] ? exc_page_fault+0x62/0x150 [74830.697225] ? asm_exc_page_fault+0x22/0x30 [74830.698344] ? rpfilter_mt+0x44/0x15e [ipt_rpfilter] [74830.699540] ipt_do_table+0x286/0x710 [ip_tables] [74830.700758] ? ip6_route_input+0x19d/0x240 [74830.701752] nf_hook_slow+0x3f/0xb0 [74830.702678] input_action_end_dx4+0x19b/0x1e0 [74830.703735] ? input_action_end_t+0xe0/0xe0 [74830.704734] seg6_local_input_core+0x2d/0x60 [74830.705782] lwtunnel_input+0x5b/0xb0 [74830.706690] __netif_receive_skb_one_core+0x63/0xa0 [74830.707825] process_backlog+0x99/0x140 [74830.709538] __napi_poll+0x2c/0x160 [74830.710673] net_rx_action+0x296/0x350 [74830.711860] __do_softirq+0xcb/0x2ac [74830.713049] do_softirq+0x63/0x90 input_action_end_dx4() passing a NULL indev to NF_HOOK(), and finally trigger a NULL dereference in rpfilter_mt()->rpfilter_is_loopback(): static bool rpfilter_is_loopback(const struct sk_buff *skb, const struct net_device *in) { // in is NULL return skb->pkt_type == PACKET_LOOPBACK || in->flags & IFF_LOOPBACK; }	5.5	More Details
CVE-2022-48846	In the Linux kernel, the following vulnerability has been resolved: block: release rq qos structures for queue without disk blkcg_init_queue() may add rq qos structures to request queue, previously blk_cleanup_queue() calls rq_qos_exit() to release them, but commit 8e141f9eb803 ("block: drain file system I/O on del_gendisk") moves rq_qos_exit() into del_gendisk(), so memory leak is caused because queues may not have disk, such as un-present scsi luns, nvme admin queue, ... Fixes the issue by adding rq_qos_exit() to blk_cleanup_queue() back. BTW, v5.18 won't need this patch any more since we move blkcg_init_queue()/blkcg_exit_queue() into disk allocation/release handler, and patches have been in for-5.18/block.	5.5	More Details
CVE-2024-40952	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix NULL pointer dereference in ocfs2_journal_dirty() bdev->bd_super has been removed and commit 8887b94d9322 change the usage from bdev->bd_super to b_assoc_map->host->i_sb. This introduces the following NULL pointer dereference in ocfs2_journal_dirty() since b_assoc_map is still not initialized. This can be easily reproduced by running xfstests generic/186, which simulate no more credits. [134.351592] BUG: kernel NULL pointer dereference, address: 0000000000000000 ... [134.355341] RIP: 0010:ocfs2_journal_dirty+0x14f/0x160 [ocfs2] ... [134.365071] Call Trace: [134.365312] <TASK> [134.365524] ? __die_body+0x1e/0x60 [134.365868] ? page_fault_oops+0x13d/0x4f0 [134.366265] ? __pfx_bit_wait_io+0x10/0x10 [134.366659] ? schedule+0x27/0xb0 [134.366981] ? exc_page_fault+0x6a/0x140 [134.367356] ? asm_exc_page_fault+0x26/0x30 [134.367762] ? ocfs2_journal_dirty+0x14f/0x160 [ocfs2] [134.368305] ? ocfs2_journal_dirty+0x13d/0x160 [ocfs2] [134.368837] ocfs2_create_new_meta_bhs.isra.51+0x139/0x2e0 [ocfs2] [134.369454] ocfs2_grow_tree+0x688/0x8a0 [ocfs2] [134.369927] ocfs2_split_and_insert.isra.67+0x35c/0x4a0 [ocfs2] [134.370521] ocfs2_split_extent+0x314/0x4d0 [ocfs2] [134.371019] ocfs2_change_extent_flag+0x174/0x410 [ocfs2] [134.371566] ocfs2_add_refcount_flag+0x3fa/0x630 [ocfs2] [134.372117] ocfs2_reflink_remap_extent+0x21b/0x4c0 [ocfs2] [134.372994] ? inode_update_timestamps+0x4a/0x120 [134.373692] ? __pfx_ocfs2_journal_access_di+0x10/0x10 [ocfs2] [134.374545] ? __pfx_ocfs2_journal_access_di+0x10/0x10 [ocfs2] [134.375393] ocfs2_reflink_remap_blocks+0xe4/0x4e0 [ocfs2] [134.376197] ocfs2_remap_file_range+0x1de/0x390 [ocfs2] [134.376971] ? security_file_permission+0x29/0x50 [134.377644] vfs_clone_file_range+0xfe/0x320 [134.378268] ioctl_file_clone+0x45/0xa0 [134.378853] do_vfs_ioctl+0x457/0x990 [134.379422] __x64_sys_ioctl+0x6e/0xd0 [134.379987] do_syscall_64+0x5d/0x170 [134.380550] entry_SYSCALL_64_after_hwframe+0x76/0x7e [134.381231] RIP: 0033:0x7fa4926397cb [134.381786] Code: 73 01 c3 48 8b 0d bd 56 38 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 8d 56 38 00 f7 d8 64 89 01 48 [134.383930] RSP: 002b:00007ffc2b39f7b8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [134.384854] RAX: ffffffffffffffda RBX: 0000000000000004 RCX: 00007fa4926397cb [134.385734] RDX: 00007ffc2b39f7f0 RSI: 000000004020940d RDI: 0000000000000003 [134.386606] RBP: 0000000000000000 R08: 00111a82a4f015bb R09: 00007fa494221000 [134.387476] R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 [134.388342] R13: 0000000000f10000 R14: 0000558e844e2ac8 R15: 0000000000f10000 [134.389207] </TASK> Fix it by only aborting transaction and journal in ocfs2_journal_dirty() now, and leave ocfs2_abort() later when detecting an aborted handle, e.g. start next transaction. Also log the handle details in this case.	5.5	More Details
CVE-2022-48841	In the Linux kernel, the following vulnerability has been resolved: ice: fix NULL pointer dereference in ice_update_vsi_tx_ring_stats() It is possible to do NULL pointer dereference in routine that updates Tx ring stats. Currently only stats and bytes are updated when ring pointer is valid, but later on ring is accessed to propagate gathered Tx stats onto VSI stats. Change the existing logic to move to next ring when ring is NULL.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40961	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible NULL deref in fib6_nh_init() syzbot reminds us that in6_dev_get() can return NULL. fib6_nh_init() ip6_validate_gw(&idev) ip6_route_check_nh(idev) *idev = in6_dev_get(dev); // can be NULL Oops: general protection fault, probably for non-canonical address 0xdfffffc00000000bc: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x00000000000005e0-0x00000000000005e7] CPU: 0 PID: 11237 Comm: syz-executor.3 Not tainted 6.10.0-rc2-syzkaller-00249-gbe27b8965297 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 RIP: 0010:fib6_nh_init+0x640/0x2160 net/ipv6/route.c:3606 Code: 00 00 fc ff df 4c 8b 64 24 58 48 8b 44 24 28 4c 8b 74 24 30 48 89 c1 48 89 44 24 28 48 8d 98 e0 05 00 00 48 89 d8 48 c1 e8 03 <42> 0f b6 04 38 84 c0 0f 85 b3 17 00 00 8b 1b 31 ff 89 de e8 b8 8b RSP: 0018:ffffc900032775a0 EFLAGS: 00010202 RAX: 00000000000000bc RBX: 00000000000005e0 RCX: 0000000000000000 RDX: 0000000000000010 RSI: ffffc90003277a54 RDI: ffff88802b3a08d8 RBP: ffffc900032778b0 R08: 00000000000002fc R09: 0000000000000000 R10: 00000000000002fc R11: 0000000000000000 R12: ffff88802b3a08b8 R13: 1ffff9200064eec8 R14: ffffc90003277a00 R15: dfffffc0000000000 FS: 00007f940feb06c0(0000) GS:ffff8880b9400000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000000245e8000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ip6_route_info_create+0x99e/0x12b0 net/ipv6/route.c:3809 ip6_route_add+0x28/0x160 net/ipv6/route.c:3853 ipv6_route_ioctl+0x588/0x870 net/ipv6/route.c:4483 inet6_ioctl+0x21a/0x280 net/ipv6/af_inet6.c:579 sock_do_ioctl+0x158/0x460 net/socket.c:1222 sock_ioctl+0x629/0x8e0 net/socket.c:1341 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:907 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:893 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f940f07cea9	5.5	More Details
CVE-2022-48845	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following: [0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ------------[cut here]------------ [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f [0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000 83070bf4 00000001 830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x60/0x80 [0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt+0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting+0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140 [0.048510] [<8108d914>] notify_cpu_starting+0x94/0x140 [0.048523] [<8106593c>] start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done. ...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them: [0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef	5.5	More Details
CVE-2022-48844	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Fix leaking sent_cmd skb sent_cmd memory is not freed before freeing hci_dev causing it to leak it contents.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40955	In the Linux kernel, the following vulnerability has been resolved: ext4: fix slab-out-of-bounds in ext4_mb_find_good_group_avg_frag_lists() We can trigger a slab-out-of-bounds with the following commands: mkfs.ext4 -F /dev/$disk 10G mount /dev/$disk /tmp/test echo 2147483647 > /sys/fs/ext4/$disk/mb_group_prealloc echo test > /tmp/test/file && sync == BUG: KASAN: slab-out-of-bounds in ext4_mb_find_good_group_avg_frag_lists+0x8a/0x200 [ext4] Read of size 8 at addr ffff888121b9d0f0 by task kworker/u2:0/11 CPU: 0 PID: 11 Comm: kworker/u2:0 Tainted: GL 6.7.0-next-20240118 #521 Call Trace: dump_stack_lvl+0x2c/0x50 kasan_report+0xb6/0xf0 ext4_mb_find_good_group_avg_frag_lists+0x8a/0x200 [ext4] ext4_mb_regular_allocator+0x19e9/0x2370 [ext4] ext4_mb_new_blocks+0x88a/0x1370 [ext4] ext4_ext_map_blocks+0x14f7/0x2390 [ext4] ext4_map_blocks+0x569/0xea0 [ext4] ext4_do_writepages+0x10f6/0x1bc0 [ext4] [...] == The flow of issue triggering is as follows: // Set s_mb_group_prealloc to 2147483647 via sysfs ext4_mb_new_blocks ext4_mb_normalize_request ext4_mb_normalize_group_request ac->ac_g_ex.fe_len = EXT4_SB(sb)->s_mb_group_prealloc ext4_mb_regular_allocator ext4_mb_choose_next_group ext4_mb_choose_next_group_best_avail mb_avg_fragment_size_order order = fls(len) - 2 = 29 ext4_mb_find_good_group_avg_frag_lists frag_list = &sbi->s_mb_avg_fragment_size[order] if (list_empty(frag_list)) // Trigger SOOB! At 4k block size, the length of the s_mb_avg_fragment_size list is 14, but an oversized s_mb_group_prealloc is set, causing slab-out-of-bounds to be triggered by an attempt to access an element at index 29. Add a new attr_id attr_clusters_in_group with values in the range [0, sbi->s_clusters_per_group] and declare mb_group_prealloc as that type to fix the issue. In addition avoid returning an order from mb_avg_fragment_size_order() greater than MB_NUM_ORDERS(sb) and reduce some useless loops.	5.5	More Details
CVE-2022-48843	In the Linux kernel, the following vulnerability has been resolved: drm/vrr: Set VRR capable prop only if it is attached to connector VRR capable property is not attached by default to the connector It is attached only if VRR is supported. So if the driver tries to call drm core set prop function without it being attached that causes NULL dereference.	5.5	More Details
CVE-2024-40960	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent possible NULL dereference in rt6_probe() syzbot caught a NULL dereference in rt6_probe() [1] Bail out if __in6_dev_get() returns NULL. [1] Oops: general protection fault, probably for non-canonical address 0xdfffffc00000000cb: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000658-0x000000000000065f] CPU: 1 PID: 22444 Comm: syz-executor.0 Not tainted 6.10.0-rc2-syzkaller-00383-gb8481381d4e2 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/02/2024 RIP: 0010:rt6_probe net/ipv6/route.c:656 [inline] RIP: 0010:find_match+0x8c4/0xf50 net/ipv6/route.c:758 Code: 14 fd f7 48 8b 85 38 ff ff ff 48 c7 45 b0 00 00 00 00 48 8d b8 5c 06 00 00 48 b8 00 00 00 00 00 fc ff df 48 89 fa 48 c1 ea 03 <0f> b6 14 02 48 89 f8 83 e0 07 83 c0 03 38 d0 7c 08 84 d2 0f 85 19 RSP: 0018:ffffc900034af070 EFLAGS: 00010203 RAX: dfffffc0000000000 RBX: 0000000000000000 RCX: ffffc90004521000 RDX: 00000000000000cb RSI: ffffffff8990d0cd RDI: 000000000000065c RBP: ffffc900034af150 R08: 0000000000000005 R09: 0000000000000000 R10: 0000000000000001 R11: 0000000000000002 R12: 000000000000000a R13: 1ffff92000695e18 R14: ffff8880244a1d20 R15: 0000000000000000 FS: 00007f4844a5a6c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000001b31b27000 CR3: 000000002d42c000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> rt6_nh_find_match+0xfa/0x1a0 net/ipv6/route.c:784 nexthop_for_each_fib6_nh+0x26d/0x4a0 net/ipv4/nexthop.c:1496 __find_rr_leaf+0x6e7/0xe00 net/ipv6/route.c:825 find_rr_leaf net/ipv6/route.c:853 [inline] rt6_select net/ipv6/route.c:897 [inline] fib6_table_lookup+0x57e/0xa30 net/ipv6/route.c:2195 ip6_pol_route+0x1cd/0x1150 net/ipv6/route.c:2231 pol_lookup_func include/net/ip6_fib.h:616 [inline] fib6_rule_lookup+0x386/0x720 net/ipv6/fib6_rules.c:121 ip6_route_output_flags_noref net/ipv6/route.c:2639 [inline] ip6_route_output_flags+0x1d0/0x640 net/ipv6/route.c:2651 ip6_dst_lookup_tail.constprop.0+0x961/0x1760 net/ipv6/ip6_output.c:1147 ip6_dst_lookup_flow+0x99/0x1d0 net/ipv6/ip6_output.c:1250 rawv6_sendmsg+0xdab/0x4340 net/ipv6/raw.c:898 inet_sendmsg+0x119/0x140 net/ipv4/af_inet.c:853 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] sock_write_iter+0x4b8/0x5c0 net/socket.c:1160 new_sync_write fs/read_write.c:497 [inline] vfs_write+0x6b6/0x1140 fs/read_write.c:590 ksys_write+0x1f8/0x260 fs/read_write.c:643 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x250 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40959	In the Linux kernel, the following vulnerability has been resolved: xfrm6: check ip6_dst_idev() return value in xfrm6_get_saddr() ip6_dst_idev() can return NULL, xfrm6_get_saddr() must act accordingly. syzbot reported: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 1 PID: 12 Comm: kworker/u8:1 Not tainted 6.10.0-rc2-syzkaller-00383-gb8481381d4e2 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/02/2024 Workqueue: wg-kex-wg1 wg_packet_handshake_send_worker RIP: 0010:xfrm6_get_saddr+0x93/0x130 net/ipv6/xfrm6_policy.c:64 Code: df 48 89 fa 48 c1 ea 03 80 3c 02 00 0f 85 97 00 00 00 4c 8b ab d8 00 00 00 48 b8 00 00 00 00 00 fc ff df 4c 89 ea 48 c1 ea 03 <80> 3c 02 00 0f 85 86 00 00 00 4d 8b 6d 00 e8 ca 13 47 01 48 b8 00 RSP: 0018:ffffc90000117378 EFLAGS: 00010246 RAX: dffffc0000000000 RBX: ffff88807b079dc0 RCX: ffffffff89a0d6d7 RDX: 0000000000000000 RSI: ffffffff89a0d6e9 RDI: ffff88807b079e98 RBP: ffff88807ad73248 R08: 0000000000000007 R09: fffffffffffff000 R10: ffff88807b079dc0 R11: 0000000000000007 R12: ffffc90000117480 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 0000000000000000(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f4586d00440 CR3: 0000000079042000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> xfrm_get_saddr net/xfrm/xfrm_policy.c:2452 [inline] xfrm_tmpl_resolve_one net/xfrm/xfrm_policy.c:2481 [inline] xfrm_tmpl_resolve+0xa26/0xf10 net/xfrm/xfrm_policy.c:2541 xfrm_resolve_and_create_bundle+0x140/0x2570 net/xfrm/xfrm_policy.c:2835 xfrm_bundle_lookup net/xfrm/xfrm_policy.c:3070 [inline] xfrm_lookup_with_ifid+0x4d1/0x1e60 net/xfrm/xfrm_policy.c:3201 xfrm_lookup net/xfrm/xfrm_policy.c:3298 [inline] xfrm_lookup_route+0x3b/0x200 net/xfrm/xfrm_policy.c:3309 ip6_dst_lookup_flow+0x15c/0x1d0 net/ipv6/ip6_output.c:1256 send6+0x611/0xd20 drivers/net/wireguard/socket.c:139 wg_socket_send_skb_to_peer+0xf9/0x220 drivers/net/wireguard/socket.c:178 wg_socket_send_buffer_to_peer+0x12b/0x190 drivers/net/wireguard/socket.c:200 wg_packet_send_handshake_initiation+0x227/0x360 drivers/net/wireguard/send.c:40 wg_packet_handshake_send_worker+0x1c/0x30 drivers/net/wireguard/send.c:51 process_one_work+0x9fb/0x1b60 kernel/workqueue.c:3231 process_scheduled_works kernel/workqueue.c:3312 [inline] worker_thread+0x6c8/0xf70 kernel/workqueue.c:3393 kthread+0x2c1/0x3a0 kernel/kthread.c:389 ret_from_fork+0x45/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244	5.5	More Details
CVE-2024-40997	In the Linux kernel, the following vulnerability has been resolved: cpufreq: amd-pstate: fix memory leak on CPU EPP exit The cpudata memory from kzalloc() in amd_pstate_epp_cpu_init() is not freed in the analogous exit function, so fix that. [rjw: Subject and changelog edits]	5.5	More Details
CVE-2024-39513	An Improper Input Validation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved allows a local, low-privileged attacker to cause a Denial of Service (DoS). When a specific "clear" command is run, the Advanced Forwarding Toolkit manager (evo-aftmand-bt or evo-aftmand-zx) crashes and restarts. The crash impacts all traffic going through the FPCs, causing a DoS. Running the command repeatedly leads to a sustained DoS condition. This issue affects Junos OS Evolved: * All versions before 20.4R3-S9-EVO, * from 21.2-EVO before 21.2R3-S7-EVO, * from 21.3-EVO before 21.3R3-S5-EVO, * from 21.4-EVO before 21.4R3-S6-EVO, * from 22.1-EVO before 22.1R3-S4-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	5.5	More Details
CVE-2024-40951	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix NULL pointer dereference in ocfs2_abort_trigger() bdev->bd_super has been removed and commit 8887b94d9322 change the usage from bdev->bd_super to b_assoc_map->host->i_sb. Since ocfs2 hasn't set bh->b_assoc_map, it will trigger NULL pointer dereference when calling into ocfs2_abort_trigger(). Actually this was pointed out in history, see commit 74e364ad1b13. But I've made a mistake when reviewing commit 8887b94d9322 and then re-introduce this regression. Since we cannot revive bdev in buffer head, so fix this issue by initializing all types of ocfs2 triggers when fill super, and then get the specific ocfs2 trigger from ocfs2_caching_info when access journal. [joseph.qi@linux.alibaba.com: v2] Link: https://lkml.kernel.org/r/20240602112045.1112708-1-joseph.qi@linux.alibaba.com	5.5	More Details
CVE-2022-48861	In the Linux kernel, the following vulnerability has been resolved: vdpa: fix use-after-free on vp_vdpa_remove When vp_vdpa driver is unbind, vp_vdpa is freed in vdpa_unregister_device and then vp_vdpa->mdev.pci_dev is dereferenced in vp_modern_remove, triggering use-after-free. Call Trace of unbinding driver free vp_vdpa : do_syscall_64 vfs_write kernfs_fop_write_iter device_release_driver_internal pci_device_remove vp_vdpa_remove vdpa_unregister_device kobject_release device_release kfree Call Trace of dereference vp_vdpa->mdev.pci_dev: vp_modern_remove pci_release_selected_regions pci_release_region pci_resource_len pci_resource_end (dev)->resource[(bar)].end	5.5	More Details
CVE-2024-39733	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 295972.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48865	In the Linux kernel, the following vulnerability has been resolved: tipc: fix kernel panic when enabling bearer When enabling a bearer on a node, a kernel panic is observed: [4.498085] RIP: 0010:tipc_mon_prep+0x4e/0x130 [tipc] ... [4.520030] Call Trace: [4.520689] <IRQ> [4.521236] tipc_link_build_proto_msg+0x375/0x750 [tipc] [4.522654] tipc_link_build_state_msg+0x48/0xc0 [tipc] [4.524034] __tipc_node_link_up+0xd7/0x290 [tipc] [4.525292] tipc_rcv+0x5da/0x730 [tipc] [4.526346] ? __netif_receive_skb_core+0xb7/0xfc0 [4.527601] tipc_l2_rcv_msg+0x5e/0x90 [tipc] [4.528737] __netif_receive_skb_list_core+0x20b/0x260 [4.530068] netif_receive_skb_list_internal+0x1bf/0x2e0 [4.531450] ? dev_gro_receive+0x4c2/0x680 [4.532512] napi_complete_done+0x6f/0x180 [4.533570] virtnet_poll+0x29c/0x42e [virtio_net] ... The node in question is receiving activate messages in another thread after changing bearer status to allow message sending/ receiving in current thread: thread 1 | thread 2 -------- | -------- | tipc_enable_bearer() | test_and_set_bit_lock() | tipc_bearer_xmit_skb() | | tipc_l2_rcv_msg() | tipc_rcv() | __tipc_node_link_up() | tipc_link_build_state_msg() | tipc_link_build_proto_msg() | tipc_mon_prep() | { | ... | // null-pointer dereference | u16 gen = mon->dom_gen; | ... | } // Not being executed yet | tipc_mon_create() | { | ... | // allocate | mon = kzalloc(); | ... | } | Monitoring pointer in thread 2 is dereferenced before monitoring data is allocated in thread 1. This causes kernel panic. This commit fixes it by allocating the monitoring data before enabling the bearer to receive messages.	5.5	More Details
CVE-2024-40932	In the Linux kernel, the following vulnerability has been resolved: drm/exynos/vidi: fix memory leak in .get_modes() The duplicated EDID is never freed. Fix it.	5.5	More Details
CVE-2022-48864	In the Linux kernel, the following vulnerability has been resolved: vdpa/mlx5: add validation for VIRTIO_NET_CTRL_MQ_VQ_PAIRS_SET command When control vq receives a VIRTIO_NET_CTRL_MQ_VQ_PAIRS_SET command request from the driver, presently there is no validation against the number of queue pairs to configure, or even if multiqueue had been negotiated or not is unverified. This may lead to kernel panic due to uninitialized resource for the queues were there any bogus request sent down by untrusted driver. Tie up the loose ends there.	5.5	More Details
CVE-2022-48863	In the Linux kernel, the following vulnerability has been resolved: mISDN: Fix memory leak in dsp_pipeline_build() dsp_pipeline_build() allocates dup pointer by kstrdup(cfg), but then it updates dup variable by strsep(&dup, "|"). As a result when it calls kfree(dup), the dup variable contains NULL. Found by Linux Driver Verification project (linuxtesting.org) with SVACE.	5.5	More Details
CVE-2022-48862	In the Linux kernel, the following vulnerability has been resolved: vhost: fix hung thread due to erroneous iotlb entries In vhost_iotlb_add_range_ctx(), range size can overflow to 0 when start is 0 and last is ULONG_MAX. One instance where it can happen is when userspace sends an IOTLB message with iova=size=uaddr=0 (vhost_process_iotlb_msg). So, an entry with size = 0, start = 0, last = ULONG_MAX ends up in the iotlb. Next time a packet is sent, iotlb_access_ok() loops indefinitely due to that erroneous entry. Call Trace: <TASK> iotlb_access_ok+0x21b/0x3e0 drivers/vhost/vhost.c:1340 vq_meta_prefetch+0xbc/0x280 drivers/vhost/vhost.c:1366 vhost_transport_do_send_pkt+0xe0/0xfd0 drivers/vhost/vsock.c:104 vhost_worker+0x23d/0x3d0 drivers/vhost/vhost.c:372 kthread+0x2e9/0x3a0 kernel/kthread.c:377 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK> Reported by syzbot at: https://syzkaller.appspot.com/bug?extid=0abd373e2e50d704db87 To fix this, do two things: 1. Return -EINVAL in vhost_chr_write_iter() when userspace asks to map a range with size 0. 2. Fix vhost_iotlb_add_range_ctx() to handle the range [0, ULONG_MAX] by splitting it into two entries.	5.5	More Details
CVE-2024-6326	An exposure of sensitive information vulnerability exists in the Rockwell Automation FactoryTalk® System Service. A malicious user could exploit this vulnerability by starting a back-up or restore process, which temporarily exposes private keys, passwords, pre-shared keys, and database folders when they are temporarily copied to an interim folder. This vulnerability is due to the lack of explicit permissions set on the backup folder. If private keys are obtained by a malicious user, they could impersonate resources on the secured network.	5.5	More Details
CVE-2022-48860	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do.	5.5	More Details
CVE-2022-48849	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: bypass tiling flag check in virtual display case (v2) vkms leverages common amdgpu framebuffer creation, and also as it does not support FB modifier, there is no need to check tiling flags when initing framebuffer when virtual display is enabled. This can fix below calltrace: amdgpu 0000:00:08.0: GFX9+ requires FB check based on format modifier WARNING: CPU: 0 PID: 1023 at drivers/gpu/drm/amd/amdgpu/amdgpu_display.c:1150 amdgpu_display_framebuffer_init+0x8e7/0xb40 [amdgpu] v2: check adev->enable_virtual_display instead as vkms can be enabled in bare metal as well.	5.5	More Details
CVE-2022-48859	In the Linux kernel, the following vulnerability has been resolved: net: marvell: prestera: Add missing of_node_put() in prestera_switch_set_base_mac_addr This node pointer is returned by of_find_compatible_node() with refcount incremented. Calling of_node_put() to aovid the refcount leak.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48857	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ... Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ____kasan_kmalloc mm/kasan/common.c:515 [inline] ____kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370 ____kasan_slab_free mm/kasan/common.c:366 [inline] ____kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x626/0xcc0 drivers/base/dd.c:670	5.5	More Details
CVE-2022-48856	In the Linux kernel, the following vulnerability has been resolved: gianfar: ethtool: Fix refcount leak in gfar_get_ts_info The of_find_compatible_node() function returns a node pointer with refcount incremented, We should use of_node_put() on it when done Add the missing of_node_put() to release the refcount.	5.5	More Details
CVE-2022-48853	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce.	5.5	More Details
CVE-2024-40964	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: cs35l41: Possible null pointer dereference in cs35l41_hda_unbind() The cs35l41_hda_unbind() function clears the hda_component entry matching it's index and then dereferences the codec pointer held in the first element of the hda_component array, this is an issue when the device index was 0. Instead use the codec pointer stashed in the cs35l41_hda structure as it will still be valid.	5.5	More Details
CVE-2024-39511	An Improper Input Validation vulnerability in the 802.1X Authentication (dot1x) Daemon of Juniper Networks Junos OS allows a local, low-privileged attacker with access to the CLI to cause a Denial of Service (DoS). On running a specific operational dot1x command, the dot1x daemon crashes. An attacker can cause a sustained DoS condition by running this command repeatedly. When the crash occurs, the authentication status of any 802.1x clients is cleared, and any authorized dot1x port becomes unauthorized. The client cannot re-authenticate until the dot1x daemon restarts. This issue affects Junos OS: * All versions before 20.4R3-S10; * 21.2 versions before 21.2R3-S7; * 21.4 versions before 21.4R3-S6; * 22.1 versions before 22.1R3-S5; * 22.2 versions before 22.2R3-S3; * 22.3 versions before 22.3R3-S2; * 22.4 versions before 22.4R3-S1; * 23.2 versions before 23.2R2.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48850	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called ... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000 RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15: 0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08] mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3 #20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f #26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START| __LINK_STATE_NOCARRIER) To prevent this scenario, we also make sure that the netdevice is present.	5.5	More Details
CVE-2022-48840	In the Linux kernel, the following vulnerability has been resolved: iavf: Fix hang during reboot/shutdown Recent commit 974578017fc1 ("iavf: Add waiting so the port is initialized in remove") adds a wait-loop at the beginning of iavf_remove() to ensure that port initialization is finished prior unregistering net device. This causes a regression in reboot/shutdown scenario because in this case callback iavf_shutdown() is called and this callback detaches the device, makes it down if it is running and sets its state to __IAVF_REMOVE. Later shutdown callback of associated PF driver (e.g. ice_shutdown) is called. That callback calls among other things sriov_disable() that calls indirectly iavf_remove() (see stack trace below). As the adapter state is already __IAVF_REMOVE then the mentioned loop is end-less and shutdown process hangs. The patch fixes this by checking adapter's state at the beginning of iavf_remove() and skips the rest of the function if the adapter is already in remove state (shutdown is in progress). Reproducer: 1. Create VF on PF driven by ice or i40e driver 2. Ensure that the VF is bound to iavf driver 3. Reboot [52625.981294] sysrq: SysRq : Show Blocked State [52625.988377] task:reboot state:D stack: 0 pid:17359 ppid: 1 f2 [52625.996732] Call Trace: [52625.999187] __schedule+0x2d1/0x830 [52626.007400] schedule+0x35/0xa0 [52626.010545] schedule_hrtimeout_range_clock+0x83/0x100 [52626.020046] usleep_range+0x5b/0x80 [52626.023540] iavf_remove+0x63/0x5b0 [iavf] [52626.027645] pci_device_remove+0x3b/0xc0 [52626.031572] device_release_driver_internal+0x103/0x1f0 [52626.036805] pci_stop_bus_device+0x72/0xa0 [52626.040904] pci_stop_and_remove_bus_device+0xe/0x20 [52626.045870] pci_iov_remove_virtfn+0xba/0x120 [52626.050232] sriov_disable+0x2f/0xe0 [52626.053813] ice_free_vfs+0x7c/0x340 [ice] [52626.057946] ice_remove+0x220/0x240 [ice] [52626.061967] ice_shutdown+0x16/0x50 [ice] [52626.065987] pci_device_shutdown+0x34/0x60 [52626.070086] device_shutdown+0x165/0x1c5 [52626.074011] kernel_restart+0xe/0x30 [52626.077593] __do_sys_reboot+0x1d2/0x210 [52626.093815] do_syscall_64+0x5b/0x1a0 [52626.097483] entry_SYSCALL_64_after_hwframe+0x65/0xca	5.5	More Details
CVE-2024-40965	In the Linux kernel, the following vulnerability has been resolved: i2c: lpi2c: Avoid calling clk_get_rate during transfer Instead of repeatedly calling clk_get_rate for each transfer, lock the clock rate and cache the value. A deadlock has been observed while adding tlv320aic32x4 audio codec to the system. When this clock provider adds its clock, the clk mutex is locked already, it needs to access i2c, which in return needs the mutex for clk_get_rate as well.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40911	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: Lock wiphy in cfg80211_get_station Wiphy should be locked before calling rdev_get_station() (see lockdep assert in ieee80211_get_station()). This fixes the following kernel NULL dereference: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000050 Mem abort info: ESR = 0x0000000096000006 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault Data abort info: ISV = 0, ISS = 0x00000006 CM = 0, WnR = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=0000000003001000 [0000000000000050] pgd=0800000002dca003, p4d=0800000002dca003, pud=08000000028e9003, pmd=0000000000000000 Internal error: Oops: 0000000096000006 [#1] SMP Modules linked in: netconsole dwc3_meson_g12a dwc3_of_simple dwc3 ip_gre gre ath10k_pci ath10k_core ath9k ath9k_common ath9k_hw ath CPU: 0 PID: 1091 Comm: kworker/u8:0 Not tainted 6.4.0-02144-g565f9a3a7911-dirty #705 Hardware name: RPT (r1) (DT) Workqueue: bat_events batadv_v_elp_throughput_metric_update pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : ath10k_sta_statistics+0x10/0x2dc [ath10k_core] lr : sta_set_sinfo+0xcc/0xbd4 sp : ffff000007b43ad0 x29: ffff000007b43ad0 x28: ffff0000071fa900 x27: ffff00000294ca98 x26: ffff000006830880 x25: ffff000006830880 x24: ffff00000294c000 x23: 0000000000000001 x22: ffff000007b43c90 x21: ffff800008898acc x20: ffff00000294c6e8 x19: ffff000007b43c90 x18: 0000000000000000 x17: 445946354d552d78 x16: 62661f7200000000 x15: 57464f445946354d x14: 0000000000000000 x13: 00000000000000e3 x12: d5f0acbcebea978e x11: 00000000000000e3 x10: 000000010048fe41 x9 : 0000000000000000 x8 : ffff000007b43d90 x7 : 000000007a1e2125 x6 : 0000000000000000 x5 : ffff0000024e0900 x4 : ffff800000a0250c x3 : ffff000007b43c90 x2 : ffff00000294ca98 x1 : ffff000006831920 x0 : 0000000000000000 Call trace: ath10k_sta_statistics+0x10/0x2dc [ath10k_core] sta_set_sinfo+0xcc/0xbd4 ieee80211_get_station+0x2c/0x44 cfg80211_get_station+0x80/0x154 batadv_v_elp_get_throughput+0x138/0x1fc batadv_v_elp_throughput_metric_update+0x1c/0xa4 process_one_work+0x1ec/0x414 worker_thread+0x70/0x46c kthread+0xdc/0xe0 ret_from_fork+0x10/0x20 Code: a9bb7bfd 910003fd a90153f3 f9411c40 (f9402814) This happens because STA has time to disconnect and reconnect before batadv_v_elp_throughput_metric_update() delayed work gets scheduled. In this situation, ath10k_sta_state() can be in the middle of resetting arsta data when the work queue get chance to be scheduled and ends up accessing it. Locking wiphy prevents that.	5.5	More Details
CVE-2024-40980	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: replace spin_lock by raw_spin_lock trace_drop_common() is called with preemption disabled, and it acquires a spin_lock. This is problematic for RT kernels because spin_locks are sleeping locks in this configuration, which causes the following splat: BUG: sleeping function called from invalid context at kernel/locking/spinlock_rt.c:48 in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 449, name: rcuc/47 preempt_count: 1, expected: 0 RCU nest depth: 2, expected: 2 5 locks held by rcuc/47/449: #0: ff1100086ec30a60 ((softirq_ctrl.lock)){+.+.}-{2:2}, at: __local_bh_disable_ip+0x105/0x210 #1: ffffffffb394a280 (rcu_read_lock){....}-{1:2}, at: rt_spin_lock+0xbf/0x130 #2: ffffffffb394a280 (rcu_read_lock){....}-{1:2}, at: __local_bh_disable_ip+0x11c/0x210 #3: ffffffffb394a160 (rcu_callback){....}-{0:0}, at: rcu_do_batch+0x360/0xc70 #4: ff1100086ee07520 (&data->lock){+.+.}-{2:2}, at: trace_drop_common.constprop.0+0xb5/0x290 irq event stamp: 139909 hardirqs last enabled at (139908): [<ffffffffb1df2b33>] _raw_spin_unlock_irqrestore+0x63/0x80 hardirqs last disabled at (139909): [<ffffffffb19bd03d>] trace_drop_common.constprop.0+0x26d/0x290 softirqs last enabled at (139892): [<ffffffffb07a1083>] __local_bh_enable_ip+0x103/0x170 softirqs last disabled at (139898): [<ffffffffb0909b33>] rcu_cpu_kthread+0x93/0x1f0 Preemption disabled at: [<ffffffffb1de786b>] rt_mutex_slowunlock+0xab/0x2e0 CPU: 47 PID: 449 Comm: rcuc/47 Not tainted 6.9.0-rc2-rt1+ #7 Hardware name: Dell Inc. PowerEdge R650/0Y2G81, BIOS 1.6.5 04/15/2022 Call Trace: <TASK> dump_stack_lvl+0x8c/0xd0 dump_stack+0x14/0x20 __might_resched+0x21e/0x2f0 rt_spin_lock+0x5e/0x130 ? trace_drop_common.constprop.0+0xb5/0x290 ? skb_queue_purge_reason.part.0+0x1bf/0x230 trace_drop_common.constprop.0+0xb5/0x290 ? preempt_count_sub+0x1c/0xd0 ? _raw_spin_unlock_irqrestore+0x4a/0x80 ? __pfx_trace_drop_common.constprop.0+0x10/0x10 ? rt_mutex_slowunlock+0x26a/0x2e0 ? skb_queue_purge_reason.part.0+0x1bf/0x230 ? __pfx_rt_mutex_slowunlock+0x10/0x10 ? skb_queue_purge_reason.part.0+0x1bf/0x230 trace_kfree_skb_hit+0x15/0x20 trace_kfree_skb+0xe9/0x150 kfree_skb_reason+0x7b/0x110 skb_queue_purge_reason.part.0+0x1bf/0x230 ? __pfx_skb_queue_purge_reason.part.0+0x10/0x10 ? mark_lock.part.0+0x8a/0x520 ... trace_drop_common() also disables interrupts, but this is a minor issue because we could easily replace it with a local_lock. Replace the spin_lock with raw_spin_lock to avoid sleeping in atomic context.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48839	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg() syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations, tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline] packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ____sys_recvmsg+0x2c4/0x600 net/socket.c:2632 ___sys_recvmsg+0x127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 0000000020000500 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ____sys_recvmsg+0x0/0x600 include/linux/uio.h:246 this frame has 1 object: [32, 160) 'addr' Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 >ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ==	5.5	More Details
CVE-2024-40982	In the Linux kernel, the following vulnerability has been resolved: ssb: Fix potential NULL pointer dereference in ssb_device_uevent() The ssb_device_uevent() function first attempts to convert the 'dev' pointer to 'struct ssb_device *'. However, it mistakenly dereferences 'dev' before performing the NULL check, potentially leading to a NULL pointer dereference if 'dev' is NULL. To fix this issue, move the NULL check before dereferencing the 'dev' pointer, ensuring that the pointer is valid before attempting to use it. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details
CVE-2024-21161	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.20. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Linux hosts only. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2024-21163	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	5.5	More Details
CVE-2024-40910	In the Linux kernel, the following vulnerability has been resolved: ax25: Fix refcount imbalance on inbound connections When releasing a socket in ax25_release(), we call netdev_put() to decrease the refcount on the associated ax.25 device. However, the execution path for accepting an incoming connection never calls netdev_hold(). This imbalance leads to refcount errors, and ultimately to kernel crashes. A typical call trace for the above situation will start with one of the following errors: refcount_t: decrement hit 0; leaking memory. refcount_t: underflow; use-after-free. And will then have a trace like: Call Trace: <TASK> ? show_regs+0x64/0x70 ? __warn+0x83/0x120 ? refcount_warn_saturate+0xb2/0x100 ? report_bug+0x158/0x190 ? prb_read_valid+0x20/0x30 ? handle_bug+0x3e/0x70 ? exc_invalid_op+0x1c/0x70 ? asm_exc_invalid_op+0x1f/0x30 ? refcount_warn_saturate+0xb2/0x100 ? refcount_warn_saturate+0xb2/0x100 ax25_release+0x2ad/0x360 __sock_release+0x35/0xa0 sock_close+0x19/0x20 [...] On reboot (or any attempt to remove the interface), the kernel gets stuck in an infinite loop: unregister_netdevice: waiting for ax0 to become free. Usage count = 0 This patch corrects these issues by ensuring that we call netdev_hold() and ax25_dev_hold() for new connections in ax25_accept(). This makes the logic leading to ax25_accept() match the logic for ax25_bind(): in both cases we increment the refcount, which is ultimately decremented in ax25_release().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40907	In the Linux kernel, the following vulnerability has been resolved: ionic: fix kernel panic in XDP_TX action In the XDP_TX path, ionic driver sends a packet to the TX path with rx page and corresponding dma address. After tx is done, ionic_tx_clean() frees that page. But RX ring buffer isn't reset to NULL. So, it uses a freed page, which causes kernel panic. BUG: unable to handle page fault for address: ffff8881576c110c PGD 773801067 P4D 773801067 PUD 87f086067 PMD 87efca067 PTE 800ffffea893e060 Oops: Oops: 0000 [#1] PREEMPT SMP DEBUG_PAGEALLOC KASAN NOPTI CPU: 1 PID: 25 Comm: ksoftirqd/1 Not tainted 6.9.0+ #11 Hardware name: ASUS System Product Name/PRIME Z690-P D4, BIOS 0603 11/01/2021 RIP: 0010:bpf_prog_f0b8caeac1068a55_balancer_ingress+0x3b/0x44f Code: 00 53 41 55 41 56 41 57 b8 01 00 00 00 48 8b 5f 08 4c 8b 77 00 4c 89 f7 48 83 c7 0e 48 39 d8 RSP: 0018:ffff888104e6fa28 EFLAGS: 00010283 RAX: 0000000000000002 RBX: ffff8881576c1140 RCX: 0000000000000002 RDX: ffffffffc0051f64 RSI: ffffc90002d33048 RDI: ffff8881576c110e RBP: ffff888104e6fa88 R08: 0000000000000000 R09: ffffed1027a04a23 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8881b03a21a8 R13: ffff8881589f800f R14: ffff8881576c1100 R15: 00000001576c1100 FS: 0000000000000000(0000) GS:ffff88881ae00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffff8881576c110c CR3: 0000000767a90000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x254/0x790 ? __pfx_page_fault_oops+0x10/0x10 ? __pfx_is_prefetch.constprop.0+0x10/0x10 ? search_bpf_extables+0x165/0x260 ? fixup_exception+0x4a/0x970 ? exc_page_fault+0xcb/0xe0 ? asm_exc_page_fault+0x22/0x30 ? 0xffffffffc0051f64 ? bpf_prog_f0b8caeac1068a55_balancer_ingress+0x3b/0x44f ? do_raw_spin_unlock+0x54/0x220 ionic_rx_service+0x11ab/0x3010 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ? ionic_tx_clean+0x29b/0xc60 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ? __pfx_ionic_tx_clean+0x10/0x10 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ? __pfx_ionic_rx_service+0x10/0x10 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ? ionic_tx_cq_service+0x25d/0xa00 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ? __pfx_ionic_rx_service+0x10/0x10 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ionic_cq_service+0x69/0x150 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] ionic_txrx_napi+0x11a/0x540 [ionic 9180c3001ab627d82bbc5f3ebe8a0decaf6bb864] __napi_poll.constprop.0+0xa0/0x440 net_rx_action+0x7e7/0xc30 ? __pfx_net_rx_action+0x10/0x10	5.5	More Details
CVE-2024-40904	In the Linux kernel, the following vulnerability has been resolved: USB: class: cdc-wdm: Fix CPU lockup caused by excessive log messages The syzbot fuzzer found that the interrupt-URB completion callback in the cdc-wdm driver was taking too long, and the driver's immediate resubmission of interrupt URBs with -EPROTO status combined with the dummy-hcd emulation to cause a CPU lockup: cdc_wdm 1-1:1.0: nonzero urb status received: -71 cdc_wdm 1-1:1.0: wdm_int_callback - 0 bytes watchdog: BUG: soft lockup - CPU#0 stuck for 26s! [syz-executor782:6625] CPU#0 Utilization every 4s during lockup: #1: 98% system, 0% softirq, 3% hardirq, 0% idle #2: 98% system, 0% softirq, 3% hardirq, 0% idle #3: 98% system, 0% softirq, 3% hardirq, 0% idle #4: 98% system, 0% softirq, 3% hardirq, 0% idle #5: 98% system, 1% softirq, 3% hardirq, 0% idle Modules linked in: irq event stamp: 73096 hardirqs last enabled at (73095): [<ffff80008037bc00>] console_emit_next_record kernel/printk/printk.c:2935 [inline] hardirqs last enabled at (73095): [<ffff80008037bc00>] console_flush_all+0x650/0xb74 kernel/printk/printk.c:2994 hardirqs last disabled at (73096): [<ffff80008af10b00>] __el1_irq arch/arm64/kernel/entry-common.c:533 [inline] hardirqs last disabled at (73096): [<ffff80008af10b00>] el1_interrupt+0x24/0x68 arch/arm64/kernel/entry-common.c:551 softirqs last enabled at (73048): [<ffff8000801ea530>] softirq_handle_end kernel/softirq.c:400 [inline] softirqs last enabled at (73048): [<ffff8000801ea530>] handle_softirqs+0xa60/0xc34 kernel/softirq.c:582 softirqs last disabled at (73043): [<ffff800080020de8>] __do_softirq+0x14/0x20 kernel/softirq.c:588 CPU: 0 PID: 6625 Comm: syz-executor782 Tainted: G W 6.10.0-rc2-syzkaller-g8867bbd4a056 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/02/2024 Testing showed that the problem did not occur if the two error messages -- the first two lines above -- were removed; apparently adding material to the kernel log takes a surprisingly large amount of time. In any case, the best approach for preventing these lockups and to avoid spamming the log with thousands of error messages per second is to ratelimit the two dev_err() calls. Therefore we replace them with dev_err_ratelimited().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48781	In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - get rid of alg_memory_allocated alg_memory_allocated does not seem to be really used. alg_proto does have a .memory_allocated field, but no corresponding .sysctl_mem. This means sk_has_account() returns true, but all sk_prot_mem_limits() users will trigger a NULL dereference [1]. THis was not a problem until SO_RESERVE_MEM addition. general protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] PREEMPT SMP KASAN KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f] CPU: 1 PID: 3591 Comm: syz-executor153 Not tainted 5.17.0-rc3-syzkaller-00316-gb81b1829e7e3 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:sk_prot_mem_limits include/net/sock.h:1523 [inline] RIP: 0010:sock_reserve_memory+0x1d7/0x330 net/core/sock.c:1000 Code: 08 00 74 08 48 89 ef e8 27 20 bb f9 4c 03 7c 24 10 48 8b 6d 00 48 83 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 fc ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4c 89 ff 48 RSP: 0018:ffffc90001f1fb68 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffff88814aabc000 RCX: dffffc0000000000 RDX: 0000000000000001 RSI: 0000000000000008 RDI: ffffffff90e18120 RBP: 0000000000000008 R08: dffffc0000000000 R09: fffffbfff21c3025 R10: fffffbfff21c3025 R11: 0000000000000000 R12: ffffffff8d109840 R13: 0000000000001002 R14: 0000000000000001 R15: 0000000000000001 FS: 0000555556e08300(0000) GS:ffff8880b9b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc74416f130 CR3: 0000000073d9e000 CR4: 00000000003506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> sock_setsockopt+0x14a9/0x3a30 net/core/sock.c:1446 __sys_setsockopt+0x5af/0x980 net/socket.c:2176 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xb1/0xc0 net/socket.c:2188 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x44/0xd0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fc7440fddc9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 15 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffe98f07968 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fc7440fddc9 RDX: 0000000000000049 RSI: 0000000000000001 RDI: 0000000000000004 RBP: 0000000000000000 R08: 0000000000000004 R09: 00007ffe98f07990 R10: 0000000020000000 R11: 0000000000000246 R12: 00007ffe98f0798c R13: 00007ffe98f079a0 R14: 00007ffe98f079e0 R15: 0000000000000000 </TASK> Modules linked in: ---[end trace 0000000000000000]--- RIP: 0010:sk_prot_mem_limits include/net/sock.h:1523 [inline] RIP: 0010:sock_reserve_memory+0x1d7/0x330 net/core/sock.c:1000 Code: 08 00 74 08 48 89 ef e8 27 20 bb f9 4c 03 7c 24 10 48 8b 6d 00 48 83 c5 08 48 89 e8 48 c1 e8 03 48 b9 00 00 00 00 00 fc ff df <80> 3c 08 00 74 08 48 89 ef e8 fb 1f bb f9 48 8b 6d 00 4c 89 ff 48 RSP: 0018:ffffc90001f1fb68 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffff88814aabc000 RCX: dffffc0000000000 RDX: 0000000000000001 RSI: 0000000000000008 RDI: ffffffff90e18120 RBP: 0000000000000008 R08: dffffc0000000000 R09: fffffbfff21c3025 R10: fffffbfff21c3025 R11: 0000000000000000 R12: ffffffff8d109840 R13: 0000000000001002 R14: 0000000000000001 R15: 0000000000000001 FS: 0000555556e08300(0000) GS:ffff8880b9b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc74416f130 CR3: 0000000073d9e000 CR4: 00000000003506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000	5.5	More Details
CVE-2024-6625	The WP Total Branding – Complete branding solution for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2024-39827	Improper input validation in the installer for Zoom Workplace Desktop App for Windows before version 6.0.10 may allow an authenticated user to conduct a denial of service via local access.	5.5	More Details
CVE-2022-48777	In the Linux kernel, the following vulnerability has been resolved: mtd: parsers: qcom: Fix kernel panic on skipped partition In the event of a skipped partition (case when the entry name is empty) the kernel panics in the cleanup function as the name entry is NULL. Rework the parser logic by first checking the real partition number and then allocate the space and set the data for the valid partitions. The logic was also fundamentally wrong as with a skipped partition, the parts number returned was incorrect by not decreasing it for the skipped partitions.	5.5	More Details
CVE-2022-48775	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: Fix memory leak in vmbus_add_channel_kobj kobject_init_and_add() takes reference even when it fails. According to the doc of kobject_init_and_add()： If this function returns an error, kobject_put() must be called to properly clean up the memory associated with the object. Fix memory leak by calling kobject_put().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39506	In the Linux kernel, the following vulnerability has been resolved: liquidio: Adjust a NULL pointer handling path in lio_vf_rep_copy_packet In lio_vf_rep_copy_packet() pg_info->page is compared to a NULL value, but then it is unconditionally passed to skb_add_rx_frag() which looks strange and could lead to null pointer dereference. lio_vf_rep_copy_packet() call trace looks like: octeon_droq_process_packets octeon_droq_fast_process_packets octeon_droq_dispatch_pkt octeon_create_recv_info ...search in the dispatch_list... ->disp_fn(rdisp->rinfo, ...) lio_vf_rep_pkt_recv(struct octeon_recv_info *recv_info, ...) In this path there is no code which sets pg_info->page to NULL. So this check looks unneeded and doesn't solve potential problem. But I guess the author had reason to add a check and I have no such card and can't do real test. In addition, the code in the function liquidio_push_packet() in liquidio/lio_core.c does exactly the same. Based on this, I consider the most acceptable compromise solution to adjust this issue by moving skb_add_rx_frag() into conditional scope. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details
CVE-2022-48773	In the Linux kernel, the following vulnerability has been resolved: xprtrdma: fix pointer derefs in error cases of rpcrdma_ep_create If there are failures then we must not leave the non-NULL pointers with the error value, otherwise `rpcrdma_ep_destroy` gets confused and tries free them, resulting in an Oops.	5.5	More Details
CVE-2024-41006	In the Linux kernel, the following vulnerability has been resolved: netrom: Fix a memory leak in nr_heartbeat_expiry() syzbot reported a memory leak in nr_create() [0]. Commit 409db27e3a2e ("netrom: Fix use-after-free of a listening socket.") added sock_hold() to the nr_heartbeat_expiry() function, where a) a socket has a SOCK_DESTROY flag or b) a listening socket has a SOCK_DEAD flag. But in the case "a," when the SOCK_DESTROY flag is set, the file descriptor has already been closed and the nr_release() function has been called. So it makes no sense to hold the reference count because no one will call another nr_destroy_socket() and put it as in the case "b." nr_connect nr_establish_data_link nr_start_heartbeat nr_release switch (nr->state) case NR_STATE_3 nr->state = NR_STATE_2 sock_set_flag(sk, SOCK_DESTROY); nr_rx_frame nr_process_rx_frame switch (nr->state) case NR_STATE_2 nr_state2_machine() nr_disconnect() nr_sk(sk)->state = NR_STATE_0 sock_set_flag(sk, SOCK_DEAD) nr_heartbeat_expiry switch (nr->state) case NR_STATE_0 if (sock_flag(sk, SOCK_DESTROY) || (sk->sk_state == TCP_LISTEN && sock_flag(sk, SOCK_DEAD))) sock_hold() // (!!!) nr_destroy_socket() To fix the memory leak, let's call sock_hold() only for a listening socket. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with Syzkaller. [0]: https://syzkaller.appspot.com/bug?extid=d327a1f3b12e1e206c16	5.5	More Details
CVE-2024-39504	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_inner: validate mandatory meta and payload Check for mandatory netlink attributes in payload and meta expression when used embedded from the inner expression, otherwise NULL pointer dereference is possible from userspace.	5.5	More Details
CVE-2021-47622	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: Fix a deadlock in the error handler The following deadlock has been observed on a test setup: - All tags allocated - The SCSI error handler calls ufshcd_eh_host_reset_handler() - ufshcd_eh_host_reset_handler() queues work that calls ufshcd_err_handler() - ufshcd_err_handler() locks up as follows: Workqueue: ufs_eh_wq_0 ufshcd_err_handler.cfi_jt Call trace: __switch_to+0x298/0x5d8 __schedule+0x6cc/0xa94 schedule+0x12c/0x298 blk_mq_get_tag+0x210/0x480 __blk_mq_alloc_request+0x1c8/0x284 blk_get_request+0x74/0x134 ufshcd_exec_dev_cmd+0x68/0x640 ufshcd_verify_dev_init+0x68/0x35c ufshcd_probe_hba+0x12c/0x1cb8 ufshcd_host_reset_and_restore+0x88/0x254 ufshcd_reset_and_restore+0xd0/0x354 ufshcd_err_handler+0x408/0xc58 process_one_work+0x24c/0x66c worker_thread+0x3e8/0xa4c kthread+0x150/0x1b4 ret_from_fork+0x10/0x30 Fix this lockup by making ufshcd_exec_dev_cmd() allocate a reserved request.	5.5	More Details
CVE-2024-39498	In the Linux kernel, the following vulnerability has been resolved: drm/mst: Fix NULL pointer dereference at drm_dp_add_payload_part2 [Why] Commit: - commit 5aa1dfcdf0a4 ("drm/mst: Refactor the flow for payload allocation/removement") accidently overwrite the commit - commit 54d217406afe ("drm: use mgr->dev in drm_dbg_kms in drm_dp_add_payload_part2") which cause regression. [How] Recover the original NULL fix and remove the unnecessary input parameter 'state' for drm_dp_add_payload_part2(). (cherry picked from commit 4545614c1d8da603e57b60dd66224d81b6ffc305)	5.5	More Details
CVE-2024-41002	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/sec - Fix memory leak for sec resource release The AIV is one of the SEC resources. When releasing resources, it need to release the AIV resources at the same time. Otherwise, memory leakage occurs. The aiv resource release is added to the sec resource release function.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41001	In the Linux kernel, the following vulnerability has been resolved: io_uring/sqpoll: work around a potential audit memory leak kmemleak complains that there's a memory leak related to connect handling: unreferenced object 0xffff0001093bdf00 (size 128): comm "iou-sqp-455", pid 457, jiffies 4294894164 hex dump (first 32 bytes): 02 00 fa ea 7f 00 00 01 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 2e481b1a): [<00000000c0a26af4>] kmemleak_alloc+0x30/0x38 [<000000009c30bb45>] kmalloc_trace+0x228/0x358 [<000000009da9d39f>] __audit_sockaddr+0xd0/0x138 [<0000000089a93e34>] move_addr_to_kernel+0x1a0/0x1f8 [<000000000b4e80e6>] io_connect_prep+0x1ec/0x2d4 [<00000000abfbcd99>] io_submit_sqes+0x588/0x1e48 [<00000000e7c25e07>] io_sq_thread+0x8a4/0x10e4 [<00000000d999b491>] ret_from_fork+0x10/0x20 which can can happen if: 1) The command type does something on the prep side that triggers an audit call. 2) The thread hasn't done any operations before this that triggered an audit call inside ->issue(), where we have audit_uring_entry() and audit_uring_exit(). Work around this by issuing a blanket NOP operation before the SQPOLL does anything.	5.5	More Details
CVE-2024-40995	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: fix possible infinite loop in tcf_idr_check_alloc() syzbot found hanging tasks waiting on rtnl_lock [1] A reproducer is available in the syzbot bug. When a request to add multiple actions with the same index is sent, the second request will block forever on the first request. This holds rtnl_lock, and causes tasks to hang. Return -EAGAIN to prevent infinite looping, while keeping documented behavior. [1] INFO: task kworker/1:0:5088 blocked for more than 143 seconds. Not tainted 6.9.0-rc4-syzkaller-00173-g3cdb45594619 #0 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:kworker/1:0 state:D stack:23744 pid:5088 tgid:5088 ppid:2 flags:0x00004000 Workqueue: events_power_efficient reg_check_chans_work Call Trace: <TASK> context_switch kernel/sched/core.c:5409 [inline] __schedule+0xf15/0x5d00 kernel/sched/core.c:6746 __schedule_loop kernel/sched/core.c:6823 [inline] schedule+0xe7/0x350 kernel/sched/core.c:6838 schedule_preempt_disabled+0x13/0x30 kernel/sched/core.c:6895 __mutex_lock_common kernel/locking/mutex.c:684 [inline] __mutex_lock+0x5b8/0x9c0 kernel/locking/mutex.c:752 wiphy_lock include/net/cfg80211.h:5953 [inline] reg_leave_invalid_chans net/wireless/reg.c:2466 [inline] reg_check_chans_work+0x10a/0x10e0 net/wireless/reg.c:2481	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40981	In the Linux kernel, the following vulnerability has been resolved: batman-adv: bypass empty buckets in batadv_purge_orig_ref() Many syzbot reports are pointing to soft lockups in batadv_purge_orig_ref() [1] Root cause is unknown, but we can avoid spending too much time there and perhaps get more interesting reports. [1] watchdog: BUG: soft lockup - CPU#0 stuck for 27s! [kworker/u4:6:621] Modules linked in: irq event stamp: 6182794 hardirqs last enabled at (6182793): [<ffff8000801dae10>] __local_bh_enable_ip+0x224/0x44c kernel/softirq.c:386 hardirqs last disabled at (6182794): [<ffff80008ad66a78>] __el1_irq arch/arm64/kernel/entry-common.c:533 [inline] hardirqs last disabled at (6182794): [<ffff80008ad66a78>] el1_interrupt+0x24/0x68 arch/arm64/kernel/entry-common.c:551 softirqs last enabled at (6182792): [<ffff80008aab71c4>] spin_unlock_bh include/linux/spinlock.h:396 [inline] softirqs last enabled at (6182792): [<ffff80008aab71c4>] batadv_purge_orig_ref+0x114c/0x1228 net/batman-adv/originator.c:1287 softirqs last disabled at (6182790): [<ffff80008aab61dc>] spin_lock_bh include/linux/spinlock.h:356 [inline] softirqs last disabled at (6182790): [<ffff80008aab61dc>] batadv_purge_orig_ref+0x164/0x1228 net/batman-adv/originator.c:1271 CPU: 0 PID: 621 Comm: kworker/u4:6 Not tainted 6.8.0-rc7-syzkaller-g707081b61156 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/29/2024 Workqueue: bat_events batadv_purge_orig pstate: 80400005 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : should_resched arch/arm64/include/asm/preempt.h:79 [inline] pc : __local_bh_enable_ip+0x228/0x44c kernel/softirq.c:388 lr : __local_bh_enable_ip+0x224/0x44c kernel/softirq.c:386 sp : ffff800099007970 x29: ffff800099007980 x28: 1fffe00018fce1bd x27: dfff800000000000 x26: ffff0000d2620008 x25: ffff0000c7e70de8 x24: 0000000000000001 x23: 1fffe00018e57781 x22: dfff800000000000 x21: ffff80008aab71c4 x20: ffff0001b40136c0 x19: ffff0000c72bbc08 x18: 1fffe0001a817bb0 x17: ffff800125414000 x16: ffff80008032116c x15: 0000000000000001 x14: 1fffe0001ee9d610 x13: 0000000000000000 x12: 0000000000000003 x11: 0000000000000000 x10: 0000000000ff0100 x9 : 0000000000000000 x8 : 00000000005e5789 x7 : ffff80008aab61dc x6 : 0000000000000000 x5 : 0000000000000000 x4 : 0000000000000001 x3 : 0000000000000000 x2 : 0000000000000006 x1 : 0000000000000080 x0 : ffff800125414000 Call trace: __daif_local_irq_enable arch/arm64/include/asm/irqflags.h:27 [inline] arch_local_irq_enable arch/arm64/include/asm/irqflags.h:49 [inline] __local_bh_enable_ip+0x228/0x44c kernel/softirq.c:386 __raw_spin_unlock_bh include/linux/spinlock_api_smp.h:167 [inline] _raw_spin_unlock_bh+0x3c/0x4c kernel/locking/spinlock.c:210 spin_unlock_bh include/linux/spinlock.h:396 [inline] batadv_purge_orig_ref+0x114c/0x1228 net/batman-adv/originator.c:1287 batadv_purge_orig+0x20/0x70 net/batman-adv/originator.c:1300 process_one_work+0x694/0x1204 kernel/workqueue.c:2633 process_scheduled_works kernel/workqueue.c:2706 [inline] worker_thread+0x938/0xef4 kernel/workqueue.c:2787 kthread+0x288/0x310 kernel/kthread.c:388 ret_from_fork+0x10/0x20 arch/arm64/kernel/entry.S:860 Sending NMI from CPU 0 to CPUs 1: NMI backtrace for cpu 1 CPU: 1 PID: 0 Comm: swapper/1 Not tainted 6.8.0-rc7-syzkaller-g707081b61156 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/29/2024 pstate: 80400005 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : arch_local_irq_enable+0x8/0xc arch/arm64/include/asm/irqflags.h:51 lr : default_idle_call+0xf8/0x128 kernel/sched/idle.c:103 sp : ffff800093a17d30 x29: ffff800093a17d30 x28: dfff800000000000 x27: 1ffff00012742fb4 x26: ffff80008ec9d000 x25: 0000000000000000 x24: 0000000000000002 x23: 1ffff00011d93a74 x22: ffff80008ec9d3a0 x21: 0000000000000000 x20: ffff0000c19dbc00 x19: ffff8000802d0fd8 x18: 1fffe00036804396 x17: ffff80008ec9d000 x16: ffff8000802d089c x15: 0000000000000001 ---truncated---	5.5	More Details
CVE-2024-40934	In the Linux kernel, the following vulnerability has been resolved: HID: logitech-dj: Fix memory leak in logi_dj_recv_switch_to_dj_mode() Fix a memory leak on logi_dj_recv_send_report() error path.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48835	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Page fault in reply q processing A page fault was encountered in mpt3sas on a LUN reset error path: [145.763216] mpt3sas_cm1: Task abort tm failed: handle(0x0002),timeout(30) tr_method(0x0) smid(3) msix_index(0) [145.778932] scsi 1:0:0:0: task abort: FAILED scmd(0x0000000024ba29a2) [145.817307] scsi 1:0:0:0: attempting device reset! scmd(0x0000000024ba29a2) [145.827253] scsi 1:0:0:0: [sg1] tag#2 CDB: Receive Diagnostic 1c 01 01 ff fc 00 [145.837617] scsi target1:0:0: handle(0x0002), sas_address(0x500605b0000272b9), phy(0) [145.848598] scsi target1:0:0: enclosure logical id(0x500605b0000272b8), slot(0) [149.858378] mpt3sas_cm1: Poll ReplyDescriptor queues for completion of smid(0), task_type(0x05), handle(0x0002) [149.875202] BUG: unable to handle page fault for address: 00000007fffc445d [149.885617] #PF: supervisor read access in kernel mode [149.894346] #PF: error_code(0x0000) - not-present page [149.903123] PGD 0 P4D 0 [149.909387] Oops: 0000 [#1] PREEMPT SMP NOPTI [149.917417] CPU: 24 PID: 3512 Comm: scsi_eh_1 Kdump: loaded Tainted: G S O 5.10.89-altav-1 #1 [149.934327] Hardware name: DDN 200NVX2 /200NVX2-MB , BIOS ATHG2.2.02.01 09/10/2021 [149.951871] RIP: 0010:_base_process_reply_queue+0x4b/0x900 [mpt3sas] [149.961889] Code: 0f 84 22 02 00 00 8d 48 01 49 89 fd 48 8d 57 38 f0 0f b1 4f 38 0f 85 d8 01 00 00 49 8b 45 10 45 31 e4 41 8b 55 0c 48 8d 1c d0 <0f> b6 03 83 e0 0f 3c 0f 0f 85 a2 00 00 00 e9 e6 01 00 00 0f b7 ee [149.991952] RSP: 0018:ffffc9000f1ebcb8 EFLAGS: 00010246 [150.000937] RAX: 0000000000000055 RBX: 00000007fffc445d RCX: 000000002548f071 [150.011841] RDX: 00000000ffff8881 RSI: 0000000000000001 RDI: ffff888125ed50d8 [150.022670] RBP: 0000000000000000 R08: 0000000000000000 R09: c0000000ffff7fff [150.033445] R10: ffffc9000f1ebb68 R11: ffffc9000f1ebb60 R12: 0000000000000000 [150.044204] R13: ffff888125ed50d8 R14: 0000000000000080 R15: 34cdc00034cdea80 [150.054963] FS: 0000000000000000(0000) GS:ffff88dfaf200000(0000) knlGS:0000000000000000 [150.066715] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [150.076078] CR2: 00000007fffc445d CR3: 000000012448a006 CR4: 0000000000770ee0 [150.086887] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [150.097670] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [150.108323] PKRU: 55555554 [150.114690] Call Trace: [150.120497] ? printk+0x48/0x4a [150.127049] mpt3sas_scsih_issue_tm.cold.114+0x2e/0x2b3 [mpt3sas] [150.136453] mpt3sas_scsih_issue_locked_tm+0x86/0xb0 [mpt3sas] [150.145759] scsih_dev_reset+0xea/0x300 [mpt3sas] [150.153891] scsi_eh_ready_devs+0x541/0x9e0 [scsi_mod] [150.162206] ? __scsi_host_match+0x20/0x20 [scsi_mod] [150.170406] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.178925] ? blk_mq_tagset_busy_iter+0x45/0x60 [150.186638] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.195087] scsi_error_handler+0x3a5/0x4a0 [scsi_mod] [150.203206] ? __schedule+0x1e9/0x610 [150.209783] ? scsi_eh_get_sense+0x210/0x210 [scsi_mod] [150.217924] kthread+0x12e/0x150 [150.224041] ? kthread_worker_fn+0x130/0x130 [150.231206] ret_from_fork+0x1f/0x30 This is caused by mpt3sas_base_sync_reply_irqs() using an invalid reply_q pointer outside of the list_for_each_entry() loop. At the end of the full list traversal the pointer is invalid. Move the _base_process_reply_queue() call inside of the loop.	5.5	More Details
CVE-2024-39493	In the Linux kernel, the following vulnerability has been resolved: crypto: qat - Fix ADF_DEV_RESET_SYNC memory leak Using completion_done to determine whether the caller has gone away only works after a complete call. Furthermore it's still possible that the caller has not yet called wait_for_completion, resulting in another potential UAF. Fix this by making the caller use cancel_work_sync and then freeing the memory safely.	5.5	More Details
CVE-2022-48826	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Fix deadlock on DSI device attach error DSI device attach to DSI host will be done with host device's lock held. Un-registering host in "device attach" error path (ex: probe retry) will result in deadlock with below call trace and non operational DSI display. Startup Call trace: [35.043036] rt_mutex_slowlock.constprop.21+0x184/0x1b8 [35.043048] mutex_lock_nested+0x7c/0xc8 [35.043060] device_del+0x4c/0x3e8 [35.043075] device_unregister+0x20/0x40 [35.043082] mipi_dsi_remove_device_fn+0x18/0x28 [35.043093] device_for_each_child+0x68/0xb0 [35.043105] mipi_dsi_host_unregister+0x40/0x90 [35.043115] vc4_dsi_host_attach+0xf0/0x120 [vc4] [35.043199] mipi_dsi_attach+0x30/0x48 [35.043209] tc358762_probe+0x128/0x164 [tc358762] [35.043225] mipi_dsi_drv_probe+0x28/0x38 [35.043234] really_probe+0xc0/0x318 [35.043244] __driver_probe_device+0x80/0xe8 [35.043254] driver_probe_device+0xb8/0x118 [35.043263] __device_attach_driver+0x98/0xe8 [35.043273] bus_for_each_drv+0x84/0xd8 [35.043281] __device_attach+0xf0/0x150 [35.043290] device_initial_probe+0x1c/0x28 [35.043300] bus_probe_device+0xa4/0xb0 [35.043308] deferred_probe_work_func+0xa0/0xe0 [35.043318] process_one_work+0x254/0x700 [35.043330] worker_thread+0x4c/0x448 [35.043339] kthread+0x19c/0x1a8 [35.043348] ret_from_fork+0x10/0x20 Shutdown Call trace: [365.565417] Call trace: [365.565423] __switch_to+0x148/0x200 [365.565452] __schedule+0x340/0x9c8 [365.565467] schedule+0x48/0x110 [365.565479] schedule_timeout+0x3b0/0x448 [365.565496] wait_for_completion+0xac/0x138 [365.565509] __flush_work+0x218/0x4e0 [365.565523] flush_work+0x1c/0x28 [365.565536] wait_for_device_probe+0x68/0x158 [365.565550] device_shutdown+0x24/0x348 [365.565561] kernel_restart_prepare+0x40/0x50 [365.565578] kernel_restart+0x20/0x70 [365.565591] __do_sys_reboot+0x10c/0x220 [365.565605] __arm64_sys_reboot+0x2c/0x38 [365.565619] invoke_syscall+0x4c/0x110 [365.565634] el0_svc_common.constprop.3+0xfc/0x120 [365.565648] do_el0_svc+0x2c/0x90 [365.565661] el0_svc+0x4c/0xf0 [365.565671] el0t_64_sync_handler+0x90/0xb8 [365.565682] el0t_64_sync+0x180/0x184	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39489	In the Linux kernel, the following vulnerability has been resolved: ipv6: sr: fix memleak in seg6_hmac_init_algo seg6_hmac_init_algo returns without cleaning up the previous allocations if one fails, so it's going to leak all that memory and the crypto tfms. Update seg6_hmac_exit to only free the memory when allocated, so we can reuse the code directly.	5.5	More Details
CVE-2024-40970	In the Linux kernel, the following vulnerability has been resolved: Avoid hw_desc array overrun in dw-axi-dmac I have a use case where nr_buffers = 3 and in which each descriptor is composed by 3 segments, resulting in the DMA channel descs_allocated to be 9. Since axi_desc_put() handles the hw_desc considering the descs_allocated, this scenario would result in a kernel panic (hw_desc array will be overrun). To fix this, the proposal is to add a new member to the axi_dma_desc structure, where we keep the number of allocated hw_descs (axi_desc_alloc()) and use it in axi_desc_put() to handle the hw_desc array correctly. Additionally I propose to remove the axi_chan_start_first_queued() call after completing the transfer, since it was identified that unbalance can occur (started descriptors can be interrupted and transfer ignored due to DMA channel not being enabled).	5.5	More Details
CVE-2024-40967	In the Linux kernel, the following vulnerability has been resolved: serial: imx: Introduce timeout when waiting on transmitter empty By waiting at most 1 second for USR2_TXDC to be set, we avoid a potential deadlock. In case of the timeout, there is not much we can do, so we simply ignore the transmitter state and optimistically try to continue.	5.5	More Details
CVE-2022-48824	In the Linux kernel, the following vulnerability has been resolved: scsi: myrs: Fix crash in error case In myrs_detect(), cs->disable_intr is NULL when privdata->hw_init() fails with non-zero. In this case, myrs_cleanup(cs) will call a NULL ptr and crash the kernel. [1.105606] myrs 0000:00:03.0: Unknown Initialization Error 5A [1.105872] myrs 0000:00:03.0: Failed to initialize Controller [1.106082] BUG: kernel NULL pointer dereference, address: 0000000000000000 [1.110774] Call Trace: [1.110950] myrs_cleanup+0xe4/0x150 [myrs] [1.111135] myrs_probe.cold+0x91/0x56a [myrs] [1.111302] ? DAC960_GEM_intr_handler+0x1f0/0x1f0 [myrs] [1.111500] local_pci_probe+0x48/0x90	5.5	More Details
CVE-2024-40912	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: Fix deadlock in ieee80211_sta_ps_deliver_wakeup() The ieee80211_sta_ps_deliver_wakeup() function takes sta->ps_lock to synchronizes with ieee80211_tx_h_unicast_ps_buf() which is called from softirq context. However using only spin_lock() to get sta->ps_lock in ieee80211_sta_ps_deliver_wakeup() does not prevent softirq to execute on this same CPU, to run ieee80211_tx_h_unicast_ps_buf() and try to take this same lock ending in deadlock. Below is an example of rcu stall that arises in such situation. rcu: INFO: rcu_sched self-detected stall on CPU rcu: 2-....: (42413413 ticks this GP) idle=b154/1/0x4000000000000000 softirq=1763/1765 fqs=21206996 rcu: (t=42586894 jiffies g=2057 q=362405 ncpus=4) CPU: 2 PID: 719 Comm: wpa_supplicant Tainted: G W 6.4.0-02158-g1b062f552873 #742 Hardware name: RPT (r1) (DT) pstate: 00000005 (nzcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : queued_spin_lock_slowpath+0x58/0x2d0 lr : invoke_tx_handlers_early+0x5b4/0x5c0 sp : ffff00001ef64660 x29: ffff00001ef64660 x28: ffff000009bc1070 x27: ffff000009bc0ad8 x26: ffff000009bc0900 x25: ffff00001ef647a8 x24: 0000000000000000 x23: ffff000009bc0900 x22: ffff000009bc0900 x21: ffff00000ac0e000 x20: ffff00000a279e00 x19: ffff00001ef646e8 x18: 0000000000000000 x17: ffff800016468000 x16: ffff00001ef608c0 x15: 0010533c93f64f80 x14: 0010395c9faa3946 x13: 0000000000000000 x12: 00000000fa83b2da x11: 000000012edeceea x10: ffff0000010fbe00 x9 : 0000000000895440 x8 : 000000000010533c x7 : ffff00000ad8b740 x6 : ffff00000c350880 x5 : 0000000000000007 x4 : 0000000000000001 x3 : 0000000000000000 x2 : 0000000000000000 x1 : 0000000000000001 x0 : ffff00000ac0e0e8 Call trace: queued_spin_lock_slowpath+0x58/0x2d0 ieee80211_tx+0x80/0x12c ieee80211_tx_pending+0x110/0x278 tasklet_action_common.constprop.0+0x10c/0x144 tasklet_action+0x20/0x28 _stext+0x11c/0x284 ____do_softirq+0xc/0x14 call_on_irq_stack+0x24/0x34 do_softirq_own_stack+0x18/0x20 do_softirq+0x74/0x7c __local_bh_enable_ip+0xa0/0xa4 _ieee80211_wake_txqs+0x3b0/0x4b8 __ieee80211_wake_queue+0x12c/0x168 ieee80211_add_pending_skbs+0xec/0x138 ieee80211_sta_ps_deliver_wakeup+0x2a4/0x480 ieee80211_mps_sta_status_update.part.0+0xd8/0x11c ieee80211_mps_sta_status_update+0x18/0x24 sta_apply_parameters+0x3bc/0x4c0 ieee80211_change_station+0x1b8/0x2dc nl80211_set_station+0x444/0x49c genl_family_rcv_msg_doit.isra.0+0xa4/0xfc genl_rcv_msg+0x1b0/0x244 netlink_rcv_skb+0x38/0x10c genl_rcv+0x34/0x48 netlink_unicast+0x254/0x2bc netlink_sendmsg+0x190/0x3b4 ____sys_sendmsg+0x1e8/0x218 ___sys_sendmsg+0x68/0x8c __sys_sendmsg+0x44/0x84 __arm64_sys_sendmsg+0x20/0x28 do_el0_svc+0x6c/0xe8 el0_svc+0x14/0x48 el0t_64_sync_handler+0xb0/0xb4 el0t_64_sync+0x14c/0x150 Using spin_lock_bh()/spin_unlock_bh() instead prevents softirq to raise on the same CPU that is holding the lock.	5.5	More Details
CVE-2022-48809	In the Linux kernel, the following vulnerability has been resolved: net: fix a memleak when uncloning an skb dst and its metadata When uncloning an skb dst and its associated metadata, a new dst+metadata is allocated and later replaces the old one in the skb. This is helpful to have a non-shared dst+metadata attached to a specific skb. The issue is the uncloned dst+metadata is initialized with a refcount of 1, which is increased to 2 before attaching it to the skb. When tun_dst_unclone returns, the dst+metadata is only referenced from a single place (the skb) while its refcount is 2. Its refcount will never drop to 0 (when the skb is consumed), leading to a memory leak. Fix this by removing the call to dst_hold in tun_dst_unclone, as the dst+metadata refcount is already 1.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25023	IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 281429.	5.5	More Details
CVE-2024-40969	In the Linux kernel, the following vulnerability has been resolved: f2fs: don't set RO when shutting down f2fs Shutdown does not check the error of thaw_super due to readonly, which causes a deadlock like below. f2fs_ioc_shutdown(F2FS_GOING_DOWN_FULLSYNC) issue_discard_thread - bdev_freeze - freeze_super - f2fs_stop_checkpoint() - f2fs_handle_critical_error - sb_start_write - set RO - waiting - bdev_thaw - thaw_super_locked - return -EINVAL, if sb_rdonly() - f2fs_stop_discard_thread -> wait for kthread_stop(discard_thread);	5.5	More Details
CVE-2022-48836	In the Linux kernel, the following vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593	5.5	More Details
CVE-2022-48808	In the Linux kernel, the following vulnerability has been resolved: net: dsa: fix panic when DSA master device unbinds on shutdown Rafael reports that on a system with LX2160A and Marvell DSA switches, if a reboot occurs while the DSA master (dpaa2-eth) is up, the following panic can be seen: systemd-shutdown[1]: Rebooting. Unable to handle kernel paging request at virtual address 00a0000800000041 [00a0000800000041] address between user and kernel address ranges Internal error: Oops: 96000004 [#1] PREEMPT SMP CPU: 6 PID: 1 Comm: systemd-shutdow Not tainted 5.16.5-00042-g8f5585009b24 #32 pc : dsa_slave_netdevice_event+0x130/0x3e4 lr : raw_notifier_call_chain+0x50/0x6c Call trace: dsa_slave_netdevice_event+0x130/0x3e4 raw_notifier_call_chain+0x50/0x6c call_netdevice_notifiers_info+0x54/0xa0 __dev_close_many+0x50/0x130 dev_close_many+0x84/0x120 unregister_netdevice_many+0x130/0x710 unregister_netdevice_queue+0x8c/0xd0 unregister_netdev+0x20/0x30 dpaa2_eth_remove+0x68/0x190 fsl_mc_driver_remove+0x20/0x5c __device_release_driver+0x21c/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumers+0xd4/0x100 __device_release_driver+0x94/0x220 device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_device_remove+0x24/0x40 __fsl_mc_device_remove+0xc/0x20 device_for_each_child+0x58/0xa0 dprc_remove+0x90/0xb0 fsl_mc_driver_remove+0x20/0x5c __device_release_driver+0x21c/0x220 device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_bus_remove+0x80/0x100 fsl_mc_bus_shutdown+0xc/0x1c platform_shutdown+0x20/0x30 device_shutdown+0x154/0x330 __do_sys_reboot+0x1cc/0x250 __arm64_sys_reboot+0x20/0x30 invoke_syscall.constprop.0+0x4c/0xe0 do_el0_svc+0x4c/0x150 el0_svc+0x24/0xb0 el0t_64_sync_handler+0xa8/0xb0 el0t_64_sync+0x178/0x17c It can be seen from the stack trace that the problem is that the deregistration of the master causes a dev_close(), which gets notified as NETDEV_GOING_DOWN to dsa_slave_netdevice_event(). But dsa_switch_shutdown() has already run, and this has unregistered the DSA slave interfaces, and yet, the NETDEV_GOING_DOWN handler attempts to call dev_close_many() on those slave interfaces, leading to the problem. The previous attempt to avoid the NETDEV_GOING_DOWN on the master after dsa_switch_shutdown() was called seems improper. Unregistering the slave interfaces is unnecessary and unhelpful. Instead, after the slaves have stopped being uppers of the DSA master, we can now reset to NULL the master->dsa_ptr pointer, which will make DSA start ignoring all future notifier events on the master.	5.5	More Details
CVE-2024-40973	In the Linux kernel, the following vulnerability has been resolved: media: mtk-vcodec: potential null pointer deference in SCP The return value of devm_kzalloc() needs to be checked to avoid NULL pointer deference. This is similar to CVE-2022-3113.	5.5	More Details
CVE-2022-48804	In the Linux kernel, the following vulnerability has been resolved: vt_ioctl: fix array_index_nospec in vt_setactivate array_index_nospec ensures that an out-of-bounds value is set to zero on the transient path. Decreasing the value by one afterwards causes a transient integer underflow. vsa.console should be decreased first and then sanitized with array_index_nospec. Kasper Acknowledgements: Jakob Koschel, Brian Johannesmeyer, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida from the VUSec group at VU Amsterdam.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48800	In the Linux kernel, the following vulnerability has been resolved: mm: vmscan: remove deadlock due to throttling failing to make progress A soft lockup bug in kcompactd was reported in a private bugzilla with the following visible in dmesg; watchdog: BUG: soft lockup - CPU#33 stuck for 26s! [kcompactd0:479] watchdog: BUG: soft lockup - CPU#33 stuck for 52s! [kcompactd0:479] watchdog: BUG: soft lockup - CPU#33 stuck for 78s! [kcompactd0:479] watchdog: BUG: soft lockup - CPU#33 stuck for 104s! [kcompactd0:479] The machine had 256G of RAM with no swap and an earlier failed allocation indicated that node 0 where kcompactd was run was potentially unreclaimable; Node 0 active_anon:29355112kB inactive_anon:2913528kB active_file:0kB inactive_file:0kB unevictable:64kB isolated(anon):0kB isolated(file):0kB mapped:8kB dirty:0kB writeback:0kB shmem:26780kB shmem_thp: 0kB shmem_pmdmapped: 0kB anon_thp: 23480320kB writeback_tmp:0kB kernel_stack:2272kB pagetables:24500kB all_unreclaimable? yes Vlastimil Babka investigated a crash dump and found that a task migrating pages was trying to drain PCP lists; PID: 52922 TASK: ffff969f820e5000 CPU: 19 COMMAND: "kworker/u128:3" Call Trace: __schedule schedule schedule_timeout wait_for_completion __flush_work __drain_all_pages __alloc_pages_slowpath.constprop.114 __alloc_pages alloc_migration_target migrate_pages migrate_to_node do_migrate_pages cpuset_migrate_mm_workfn process_one_work worker_thread kthread ret_from_fork This failure is specific to CONFIG_PREEMPT=n builds. The root of the problem is that kcompact0 is not rescheduling on a CPU while a task that has isolated a large number of the pages from the LRU is waiting on kcompact0 to reschedule so the pages can be released. While shrink_inactive_list() only loops once around too_many_isolated, reclaim can continue without rescheduling if sc->skipped_deactivate == 1 which could happen if there was no file LRU and the inactive anon list was not low.	5.5	More Details
CVE-2022-48838	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug: BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 dev_uevent+0x712/0x780 drivers/base/core.c:2320 uevent_show+0x1b8/0x380 drivers/base/core.c:2391 dev_attr_show+0x4b/0x90 drivers/base/core.c:2094 Although the bug manifested in the driver core, the real cause was a race with the gadget core. dev_uevent() does: if (dev->driver) add_uevent_var(env, "DRIVER=%s", dev->driver->name); and between the test and the dereference of dev->driver, the gadget core sets dev->driver to NULL. The race wouldn't occur if the gadget core registered its devices on a real bus, using the standard synchronization techniques of the driver core. However, it's not necessary to make such a large change in order to fix this bug; all we need to do is make sure that udc->dev.driver is always NULL. In fact, there is no reason for udc->dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC. This patch simply removes the statements in the gadget core that touch udc->dev.driver.	5.5	More Details
CVE-2024-40977	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921s: fix potential hung tasks during chip recovery During chip recovery (e.g. chip reset), there is a possible situation that kernel worker reset_work is holding the lock and waiting for kernel thread stat_worker to be parked, while stat_worker is waiting for the release of the same lock. It causes a deadlock resulting in the dumping of hung tasks messages and possible rebooting of the device. This patch prevents the execution of stat_worker during the chip recovery.	5.5	More Details
CVE-2022-48793	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: nSVM: fix potential NULL derefernce on nested migration Turns out that due to review feedback and/or rebases I accidentally moved the call to nested_svm_load_cr3 to be too early, before the NPT is enabled, which is very wrong to do. KVM can't even access guest memory at that point as nested NPT is needed for that, and of course it won't initialize the walk_mmu, which is main issue the patch was addressing. Fix this for real.	5.5	More Details
CVE-2024-6392	The Image Optimizer, Resizer and CDN – Sirv plugin for WordPress is vulnerable to unauthorized plugin settings modification due to missing capability checks on the plugin functions in all versions up to, and including, 7.2.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the connected Sirv account to an attacker-controlled one.	5.4	More Details
CVE-2024-2430	The Website Content in Page or Post WordPress plugin before 2024.04.09 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-39737	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 296004.	5.4	More Details
CVE-2024-6742	AguardNet Technology's Space Management System does not properly filter user input, allowing remote attackers with regular privileges to inject JavaScript and perform Reflected Cross-site scripting attacks.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39739	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 296008.	5.4	More Details
CVE-2024-5811	The Simple Video Directory WordPress plugin before 1.4.4 does not sanitise and escape some of its settings, which could allow contributors and higher to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.4	More Details
CVE-2024-39735	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 296002.	5.4	More Details
CVE-2024-2640	The Watu Quiz WordPress plugin before 3.4.1.2 does not sanitise and escape some of its settings, which could allow users such as authors (if they've been authorized by admins) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	5.4	More Details
CVE-2024-6528	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim’s browser run arbitrary JavaScript when they visit a page containing the injected payload.	5.4	More Details
CVE-2023-31456	There is an SSRF vulnerability in the Fluid Topics platform that affects versions prior to 4.3, where the server can be forced to make arbitrary requests to internal and external resources by an authenticated user.	5.4	More Details
CVE-2024-21139	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Answers). Supported versions that are affected are 7.0.0.0.0, 7.6.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2024-5074	The wp-eMember WordPress plugin before 10.6.6 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	5.4	More Details
CVE-2023-35006	IBM Security QRadar EDR 3.12 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. IBM X-Force ID: 297165.	5.4	More Details
CVE-2024-27095	Decidim is a participatory democracy framework. The admin panel is subject to potential XSS attach in case the attacker manages to modify some records being uploaded to the server. This vulnerability is fixed in 0.27.6 and 0.28.1.	5.4	More Details
CVE-2024-21132	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Approvals). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Purchasing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Purchasing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Purchasing accessible data as well as unauthorized read access to a subset of Oracle Purchasing accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2024-40690	IBM InfoSphere Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 297720.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21128	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: APIs). Supported versions that are affected are 12.2.6-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data as well as unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2024-3026	The WordPress Button Plugin MaxButtons WordPress plugin before 9.7.8 does not sanitise and escape some parameters, which could allow users with a role as low as editor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2024-21122	Vulnerability in the PeopleSoft Enterprise HCM Shared Components product of Oracle PeopleSoft (component: Text Catalog). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Shared Components. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Shared Components, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Shared Components accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Shared Components accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2024-4602	The Embed Peertube Playlist WordPress plugin before 1.10 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.4	More Details
CVE-2024-36450	Cross-site scripting vulnerability exists in sysinfo.cgi of Webmin versions prior to 1.910. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the website using the product. As a result, a session ID may be obtained, a webpage may be altered, or a server may be halted.	5.4	More Details
CVE-2024-4224	An authenticated stored cross-site scripting (XSS) exists in the TP-Link TL-SG1016DE affecting version TL-SG1016DE(UN) V7.6_1.0.0 Build 20230616, which could allow an adversary to run JavaScript in an administrator's browser. This issue was fixed in TL-SG1016DE(UN) V7_1.0.1 Build 20240628.	5.4	More Details
CVE-2024-5444	The Bible Text WordPress plugin through 0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-6026	The Slider by 10Web WordPress plugin before 1.2.56 does not sanitise and escape some of its Slide options, which could allow authenticated users with access to the Sliders (by default Administrator, however this can be changed via the Slider by 10Web WordPress plugin before 1.2.56's options) and the ability to add images (Editor+) to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-4655	The Ultimate Blocks WordPress plugin before 3.1.9 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-6025	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.5 does not sanitise and escape some of its Quiz settings, which could allow contributors and higher to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-5713	The If-So Dynamic Content Personalization WordPress plugin before 1.8.0.4 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	5.4	More Details
CVE-2024-5644	The Tournamatch WordPress plugin before 4.6.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.4	More Details
CVE-2024-0619	The Payflex Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the payment_callback() function in all versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to update the status of orders, which can potentially lead to revenue loss.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6646	A vulnerability was found in Netgear WN604 up to 20240710. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /downloadFile.php of the component Web Interface. The manipulation of the argument file with the input config leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271052. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-6210	The Duplicator plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 1.5.9. This makes it possible for unauthenticated attackers to obtain the full path to instances, which they may be able to use in combination with other vulnerabilities or to simplify reconnaissance work. On its own, this information is of very limited use.	5.3	More Details
CVE-2024-38709	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Milan Petrovic GD Rating System allows PHP Local File Inclusion.This issue affects GD Rating System: from n/a through 3.6.	5.3	More Details
CVE-2024-40555	Tmall_demo v2024.07.03 was discovered to contain an arbitrary file upload vulnerability.	5.3	More Details
CVE-2024-27241	Improper input validation in some Zoom Apps and SDKs may allow an authenticated user to conduct a denial of service via network access.	5.3	More Details
CVE-2024-27090	Decidim is a participatory democracy framework, written in Ruby on Rails, originally developed for the Barcelona City government online and offline participation website. If an attacker can infer the slug or URL of an unpublished or private resource, and this resource can be embbeded (such as a Participatory Process, an Assembly, a Proposal, a Result, etc), then some data of this resource could be accessed. This vulnerability is fixed in 0.27.6.	5.3	More Details
CVE-2024-21176	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.4.0 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.3	More Details
CVE-2024-6555	The WP Popups – WordPress Popup builder plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.2.0.1. This is due the plugin utilizing mobiledetect without preventing direct access to the files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-6574	The Laposta plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.12. This is due to the plugin not preventing direct access to several test files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website. This plugin is no longer being maintained and has been closed for downloads.	5.3	More Details
CVE-2024-37504	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team FileBird Document Library.This issue affects FileBird Document Library: from n/a through 2.0.6.	5.3	More Details
CVE-2024-37498	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pauple Table & Contact Form 7 Database – Tablesome.This issue affects Table & Contact Form 7 Database – Tablesome: from n/a through 1.0.33.	5.3	More Details
CVE-2024-37270	Insertion of Sensitive Information into Log File vulnerability in TrustedLogin TrustedLogin Vendor.This issue affects TrustedLogin Vendor: from n/a before 1.1.1.	5.3	More Details
CVE-2024-6556	The SmartCrawl WordPress SEO checker, SEO analyzer, SEO optimizer plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.10.8. This is due the plugin utilizing mobiledetect without preventing direct access to the files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37205	Insertion of Sensitive Information into Log File vulnerability in SERVIT Software Solutions.This issue affects affiliate-toolkit: from n/a through 3.4.4.	5.3	More Details
CVE-2024-6570	The Glossary plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.2.26. This is due the plugin utilizing wpdesk and not preventing direct access to the test files along with display_errors being enabled. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-39912	web-auth/webauthn-lib is an open source set of PHP libraries and a Symfony bundle to allow developers to integrate that authentication mechanism into their web applications. The ProfileBasedRequestOptionsBuilder method returns allowedCredentials without any credentials if no username was found. When WebAuthn is used as the first or only authentication method, an attacker can enumerate usernames based on the absence of the `allowedCredentials` property in the assertion options response. This allows enumeration of valid or invalid usernames. By knowing which usernames are valid, attackers can focus their efforts on a smaller set of potential targets, increasing the efficiency and likelihood of successful attacks. This issue has been addressed in version 4.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-6565	The AForms — Form Builder for Price Calculator & Cost Estimation plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.2.6. This is due to the plugin utilizing the aura library and allowing direct access to the phpunit test files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2023-33860	IBM Security QRadar EDR 3.12 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 257702.	5.3	More Details
CVE-2024-6559	The Backup, Restore and Migrate WordPress Sites With the XCloner Plugin plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 4.7.3. This is due the plugin utilizing sabre without preventing direct access to the files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-21143	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: User Management). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2024-38353	CodiMD allows realtime collaborative markdown notes on all platforms. CodiMD before 2.5.4 is missing authentication and access control vulnerability allowing an unauthenticated attacker to gain unauthorised access to image data uploaded to CodiMD. CodiMD does not require valid authentication to access uploaded images or to upload new image data. An attacker who can determine an uploaded image's URL can gain unauthorised access to uploaded image data. Due to the insecure random filename generation in the underlying Formidable library, an attacker can determine the filenames for previously uploaded images and the likelihood of this issue being exploited is increased. This vulnerability is fixed in 2.5.4.	5.3	More Details
CVE-2024-6739	The session cookie in MailGates and MailAudit from Openfind does not have the HttpOnly flag enabled, allowing remote attackers to potentially steal the session cookie via XSS.	5.3	More Details
CVE-2024-6738	The tumbnail API of Tronclass from WisdomGarden lacks proper access control, allowing unauthenticated remote attackers to obtain certain specific files by modifying the URL.	5.3	More Details
CVE-2024-6554	The Branda – White Label WordPress, Custom Login Page Customizer plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.4.18. This is due the plugin utilizing composer without preventing direct access to the files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39536	A Missing Release of Memory after Effective Lifetime vulnerability in the Periodic Packet Management Daemon (ppmd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS). When a BFD session configured with authentication flaps, ppmd memory can leak. Whether the leak happens depends on a race condition which is outside the attackers control. This issue only affects BFD operating in distributed aka delegated (which is the default behavior) or inline mode. Whether the leak occurs can be monitored with the following CLI command: > show ppm request-queue FPC Pending-request fpc0 2 request-total-pending: 2 where a continuously increasing number of pending requests is indicative of the leak. This issue affects: Junos OS: * All versions before 21.2R3-S8, * 21.4 versions before 21.4R3-S7, * 22.1 versions before 22.1R3-S4, * 22.2 versions before 22.2R3-S4, * 22.3 versions before 22.3R3, * 22.4 versions before 22.4R2-S2, 22.4R3. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-EVO, * 22.4-EVO versions before 22.4R3-EVO.	5.3	More Details
CVE-2024-37151	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Mishandling of multiple fragmented packets using the same IP ID value can lead to packet reassembly failure, which can lead to policy bypass. Upgrade to 7.0.6 or 6.0.20. When using af-packet, enable `defrag` to reduce the scope of the problem.	5.3	More Details
CVE-2024-39905	Red is a fully modular Discord bot. Due to a bug in Red's Core API, 3rd-party cogs using the `@commands.can_manage_channel()` command permission check without additional permission controls may authorize a user to run a command even when that user doesn't have permissions to manage a channel. None of the core commands or core cogs are affected. The maintainers of the project are not aware of any _public_ 3rd-party cog utilizing this API at the time of writing this advisory. The problem was patched and released in version 3.5.10.	5.3	More Details
CVE-2024-39329	An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. The django.contrib.auth.backends.ModelBackend.authenticate() method allows remote attackers to enumerate users via a timing attack involving login requests for users with an unusable password.	5.3	More Details
CVE-2024-6557	The SchedulePress – Auto Post & Publish, Auto Social Share, Schedule Posts with Editorial Calendar & Missed Schedule Post Publisher plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 5.1.3. This is due the plugin utilizing the wpdeveloper library and leaving the demo files in place with display_errors on. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-6550	The Gravity Forms: Multiple Form Instances plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.1.1. This is due to the plugin leaving test files with display_errors on. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-6395	An exposure of sensitive information vulnerability in GitHub Enterprise Server would allow an attacker to enumerate the names of private repositories that utilize deploy keys. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.13.1, 3.12.6, 3.11.12, 3.10.14, and 3.9.17. This vulnerability was reported via the GitHub Bug Bounty program.	5.3	More Details
CVE-2024-39539	A Missing Release of Memory after Effective Lifetime vulnerability in Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS). In a subscriber management scenario continuous subscriber logins will trigger a memory leak and eventually lead to an FPC crash and restart. This issue affects Junos OS on MX Series: * All version before 21.2R3-S6, * 21.4 versions before 21.4R3-S6, * 22.1 versions before 22.1R3-S5, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S2, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2.	5.3	More Details
CVE-2024-6336	A Security Misconfiguration vulnerability in GitHub Enterprise Server allowed sensitive information disclosure to unauthorized users in GitHub Enterprise Server by exploiting organization ruleset feature. This attack required an organization member to explicitly change the visibility of a dependent repository from private to public. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.13.1, 3.12.6, 3.11.12, 3.10.14, and 3.9.17. This vulnerability was reported via the GitHub Bug Bounty program.	5.3	More Details
CVE-2024-5816	An Incorrect Authorization vulnerability was identified in GitHub Enterprise Server that allowed a suspended GitHub App to retain access to the repository via a scoped user access token. This was only exploitable in public repositories while private repositories were not impacted. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.9.17, 3.10.14, 3.11.12, 3.12.6, 3.13.1. This vulnerability was reported via the GitHub Bug Bounty program.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40536	Shenzhen Libituo Technology Co., Ltd LBT-T300-T400 v3.2 were discovered to contain a stack overflow via the pin_3g_code parameter in the config_3g_para function.	5.3	More Details
CVE-2023-33859	IBM Security QRadar EDR 3.12 could disclose sensitive information due to an observable login response discrepancy. IBM X-Force ID: 257697.	5.3	More Details
CVE-2024-23794	An incorrect privilege assignment vulnerability in the inline editing functionality of OTRS can lead to privilege escalation. This flaw allows an agent with read-only permissions to gain full access to a ticket. This issue arises in very rare instances when an admin has previously enabled the setting 'RequiredLock' of 'AgentFrontend::Ticket::InlineEditing::Property###Watch' in the system configuration.This issue affects OTRS: * 8.0.X * 2023.X * from 2024.X through 2024.4.x	5.2	More Details
CVE-2024-21179	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21135	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21185	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38, 8.4.1 and 9.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21125	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-5178	ServiceNow has addressed a sensitive file read vulnerability that was identified in the Washington DC, Vancouver, and Utah Now Platform releases. This vulnerability could allow an administrative user to gain unauthorized access to sensitive files on the web application server. The vulnerability is addressed in the listed patches and hot fixes, which were released during the June 2024 patching cycle. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.	4.9	More Details
CVE-2024-38360	Discourse is an open source platform for community discussion. In affected versions by creating replacement words with an almost unlimited number of characters, a moderator can reduce the availability of a Discourse instance. This issue has been addressed in stable version 3.2.3 and in current betas. Users are advised to upgrade. Users unable to upgrade may manually remove the long watched words either via SQL or Rails console.	4.9	More Details
CVE-2024-20996	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21173	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21137	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21129	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21142	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21130	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21157	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21127	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21160	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21159	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21162	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-40553	Tmall_demo v2024.07.03 was discovered to contain an arbitrary file upload via the component uploadUserHeadImage.	4.9	More Details
CVE-2024-21165	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 8.0.37 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-5257	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Developer user with `admin_compliance_framework` custom role may have been able to modify the URL for a group namespace.	4.9	More Details
CVE-2024-2696	The socialdriver-framework WordPress plugin before 2024.04.30 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3112	The Quotes and Tips by BestWebSoft WordPress plugin before 1.45 does not properly validate image files uploaded, allowing high privilege users such as admin to upload arbitrary files on the server even when they should not be allowed to (for example in multisite setup)	4.8	More Details
CVE-2024-0974	The Social Media Widget WordPress plugin before 4.0.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-21148	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).	4.8	More Details
CVE-2024-21145	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2024-4753	The WP Secure Maintenance WordPress plugin before 1.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-21140	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2024-6138	The Secure Copy Content Protection and Content Locking WordPress plugin before 4.0.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-5002	The User Submitted Posts WordPress plugin before 20240516 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-3751	The Seriously Simple Podcasting WordPress plugin before 3.3.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-6070	The If-So Dynamic Content Personalization WordPress plugin before 1.8.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5286	The wp-affiliate-platform WordPress plugin before 6.5.1 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	4.8	More Details
CVE-2024-5575	The Ditty WordPress plugin before 3.1.43 does not sanitise and escape some of its blocks' settings, which could allow high privilege users such as authors to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.7	More Details
CVE-2024-6647	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in Croogo up to 4.0.7. This affects an unknown part of the file admin/settings/settings/prefix/Theme of the component Setting Handler. The manipulation of the argument Content-Type 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 identifier VDB-271053 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2024-5032	The SULly WordPress plugin before 4.3.1 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	4.7	More Details
CVE-2024-5280	The wp-affiliate-platform WordPress plugin before 6.5.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make non-logged in users execute an XSS payload via a CSRF attack	4.7	More Details
CVE-2023-7013	Inappropriate implementation in Compositing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	4.7	More Details
CVE-2024-4217	The shortcodes-ultimate-pro WordPress plugin before 7.1.5 does not properly escape some of its shortcodes' settings, making it possible for attackers with a Contributor account to conduct Stored XSS attacks.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48842	In the Linux kernel, the following vulnerability has been resolved: ice: Fix race condition during interface enslave Commit 5dbbbd01cbba83 ("ice: Avoid RTNL lock when re-creating auxiliary device") changes a process of re-creation of aux device so ice_plug_aux_dev() is called from ice_service_task() context. This unfortunately opens a race window that can result in dead-lock when interface has left LAG and immediately enters LAG again. Reproducer: ``` #!/bin/sh ip link add lag0 type bond mode 1 miimon 100 ip link set lag0 for n in {1..10}; do echo Cycle: $n ip link set ens7f0 master lag0 sleep 1 ip link set ens7f0 nomaster done ``` This results in: [20976.208697] Workqueue: ice ice_service_task [ice] [20976.213422] Call Trace: [20976.215871] __schedule+0x2d1/0x830 [20976.219364] schedule+0x35/0xa0 [20976.222510] schedule_preempt_disabled+0xa/0x10 [20976.227043] __mutex_lock.isra.7+0x310/0x420 [20976.235071] enum_all_gids_of_dev_cb+0x1c/0x100 [ib_core] [20976.251215] ib_enum_roce_netdev+0xa4/0xe0 [ib_core] [20976.256192] ib_cache_setup_one+0x33/0xa0 [ib_core] [20976.261079] ib_register_device+0x40d/0x580 [ib_core] [20976.266139] irdma_ib_register_device+0x129/0x250 [irdma] [20976.281409] irdma_probe+0x2c1/0x360 [irdma] [20976.285691] auxiliary_bus_probe+0x45/0x70 [20976.289790] really_probe+0x1f2/0x480 [20976.298509] driver_probe_device+0x49/0xc0 [20976.302609] bus_for_each_drv+0x79/0xc0 [20976.306448] __device_attach+0xdc/0x160 [20976.310286] bus_probe_device+0x9d/0xb0 [20976.314128] device_add+0x43c/0x890 [20976.321287] __auxiliary_device_add+0x43/0x60 [20976.325644] ice_plug_aux_dev+0xb2/0x100 [ice] [20976.330109] ice_service_task+0xd0c/0xed0 [ice] [20976.342591] process_one_work+0x1a7/0x360 [20976.350536] worker_thread+0x30/0x390 [20976.358128] kthread+0x10a/0x120 [20976.365547] ret_from_fork+0x1f/0x40 ... [20976.438030] task:ip state:D stack: 0 pid:213658 ppid:213627 flags:0x00004084 [20976.446469] Call Trace: [20976.448921] __schedule+0x2d1/0x830 [20976.452414] schedule+0x35/0xa0 [20976.455559] schedule_preempt_disabled+0xa/0x10 [20976.460090] __mutex_lock.isra.7+0x310/0x420 [20976.464364] device_del+0x36/0x3c0 [20976.467772] ice_unplug_aux_dev+0x1a/0x40 [ice] [20976.472313] ice_lag_event_handler+0x2a2/0x520 [ice] [20976.477288] notifier_call_chain+0x47/0x70 [20976.481386] __netdev_upper_dev_link+0x18b/0x280 [20976.489845] bond_enslave+0xe05/0x1790 [bonding] [20976.494475] do_setlink+0x336/0xf50 [20976.502517] __rtnl_newlink+0x529/0x8b0 [20976.543441] rtnl_newlink+0x43/0x60 [20976.546934] rtnetlink_rcv_msg+0x2b1/0x360 [20976.559238] netlink_rcv_skb+0x4c/0x120 [20976.563079] netlink_unicast+0x196/0x230 [20976.567005] netlink_sendmsg+0x204/0x3d0 [20976.570930] sock_sendmsg+0x4c/0x50 [20976.574423] ____sys_sendmsg+0x1eb/0x250 [20976.586807] ___sys_sendmsg+0x7c/0xc0 [20976.606353] __sys_sendmsg+0x57/0xa0 [20976.609930] do_syscall_64+0x5b/0x1a0 [20976.613598] entry_SYSCALL_64_after_hwframe+0x65/0xca 1. Command 'ip link ... set nomaster' causes that ice_plug_aux_dev() is called from ice_service_task() context, aux device is created and associated device->lock is taken. 2. Command 'ip link ... set master...' calls ice's notifier under RTNL lock and that notifier calls ice_unplug_aux_dev(). That function tries to take aux device->lock but this is already taken by ice_plug_aux_dev() in step 1 3. Later ice_plug_aux_dev() tries to take RTNL lock but this is already taken in step 2 4. Dead-lock The patch fixes this issue by following changes: - Bit ICE_FLAG_PLUG_AUX_DEV is kept to be set during ice_plug_aux_dev() call in ice_service_task() - The bit is checked in ice_clear_rdma_cap() and only if it is not set then ice_unplug_aux_dev() is called. If it is set (in other words plugging of aux device was requested and ice_plug_aux_dev() is potentially running) then the function only clears the ---truncated---	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40905	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible race in __fib6_drop_pcpu_from() syzbot found a race in __fib6_drop_pcpu_from() [1] If compiler reads more than once (*ppcpu_rt), second read could read NULL, if another cpu clears the value in rt6_get_pcpu_route(). Add a READ_ONCE() to prevent this race. Also add rcu_read_lock()/rcu_read_unlock() because we rely on RCU protection while dereferencing pcpu_rt. [1] Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000012: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000090-0x0000000000000097] CPU: 0 PID: 7543 Comm: kworker/u8:17 Not tainted 6.10.0-rc1-syzkaller-00013-g2bfcfd584ff5 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/02/2024 Workqueue: netns cleanup_net RIP: 0010:__fib6_drop_pcpu_from.part.0+0x10a/0x370 net/ipv6/ip6_fib.c:984 Code: f8 48 c1 e8 03 80 3c 28 00 0f 85 16 02 00 00 4d 8b 3f 4d 85 ff 74 31 e8 74 a7 fa f7 49 8d bf 90 00 00 00 48 89 f8 48 c1 e8 03 <80> 3c 28 00 0f 85 1e 02 00 00 49 8b 87 90 00 00 00 48 8b 0c 24 48 RSP: 0018:ffffc900040df070 EFLAGS: 00010206 RAX: 0000000000000012 RBX: 0000000000000001 RCX: ffffffff89932e16 RDX: ffff888049dd1e00 RSI: ffffffff89932d7c RDI: 0000000000000091 RBP: dfffffc0000000000 R08: 0000000000000005 R09: 0000000000000007 R10: 0000000000000001 R11: 0000000000000006 R12: ffff88807fa080b8 R13: fffffbfff1a9a07d R14: ffffed100ff41022 R15: 0000000000000001 FS: 0000000000000000(0000) GS:ffff8880b9200000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000001b32c26000 CR3: 000000005d56e000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __fib6_drop_pcpu_from net/ipv6/ip6_fib.c:966 [inline] fib6_drop_pcpu_from net/ipv6/ip6_fib.c:1027 [inline] fib6_purge_rt+0x7f2/0x9f0 net/ipv6/ip6_fib.c:1038 fib6_del_route net/ipv6/ip6_fib.c:1998 [inline] fib6_del+0xa70/0x17b0 net/ipv6/ip6_fib.c:2043 fib6_clean_node+0x426/0x5b0 net/ipv6/ip6_fib.c:2205 fib6_walk_continue+0x44f/0x8d0 net/ipv6/ip6_fib.c:2127 fib6_walk+0x182/0x370 net/ipv6/ip6_fib.c:2175 fib6_clean_tree+0xd7/0x120 net/ipv6/ip6_fib.c:2255 __fib6_clean_all+0x100/0x2d0 net/ipv6/ip6_fib.c:2271 rt6_sync_down_dev net/ipv6/route.c:4906 [inline] rt6_disable_ip+0x7ed/0xa00 net/ipv6/route.c:4911 addrconf_ifdown.isra.0+0x117/0x1b40 net/ipv6/addrconf.c:3855 addrconf_notify+0x223/0x19e0 net/ipv6/addrconf.c:3778 notifier_call_chain+0xb9/0x410 kernel/notifier.c:93 call_netdevice_notifiers_info+0xbe/0x140 net/core/dev.c:1992 call_netdevice_notifiers_extack net/core/dev.c:2030 [inline] call_netdevice_notifiers net/core/dev.c:2044 [inline] dev_close_many+0x333/0x6a0 net/core/dev.c:1585 unregister_netdevice_many_notify+0x46d/0x19f0 net/core/dev.c:11193 unregister_netdevice_many net/core/dev.c:11276 [inline] default_device_exit_batch+0x85b/0xae0 net/core/dev.c:11759 ops_exit_list+0x128/0x180 net/core/net_namespace.c:178 cleanup_net+0x5b7/0xbf0 net/core/net_namespace.c:640 process_one_work+0x9fb/0x1b60 kernel/workqueue.c:3231 process_scheduled_works kernel/workqueue.c:3312 [inline] worker_thread+0x6c8/0xf70 kernel/workqueue.c:3393 kthread+0x2c1/0x3a0 kernel/kthread.c:389 ret_from_fork+0x45/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244	4.7	More Details
CVE-2024-21155	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: User Interface). The supported version that is affected is 8.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N).	4.7	More Details
CVE-2024-3919	The OpenPGP Form Encryption for WordPress plugin before 1.5.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	4.6	More Details
CVE-2024-23485	Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation (CWE-1304) in the Controller 6000 and 7000 can lead to secured door locks connected via Aperio Communication Hubs to momentarily allow free access. This issue affects: Gallagher Controller 6000 and 7000 9.10 prior to vCR9.10.240520a (distributed in 9.10.1268(MR1)), 9.00 prior to vCR9.00.240521a (distributed in 9.00.1990(MR3)), 8.90 prior to vCR8.90.240520a (distributed in 8.90.1947 (MR4)), 8.80 prior to vCR8.80.240520a (distributed in 8.80.1726 (MR5)), 8.70 prior to vCR8.70.240520a (distributed in 8.70.2824 (MR7)), all versions of 8.60 and prior.	4.6	More Details
CVE-2023-39327	A flaw was found in OpenJPEG. Maliciously constructed pictures can cause the program to enter a large loop and continuously print warning messages on the terminal.	4.3	More Details
CVE-2024-6398	An information disclosure vulnerability in SWG in versions 12.x prior to 12.2.10 and 11.x prior to 11.2.24 allows information stored in a customizable block page to be disclosed to third-party websites due to Same Origin Policy Bypass of browsers in certain scenarios. The risk is low, because other recommended default security policies such as URL categorization and GTI are in place in most policies to block access to uncategorized/high risk websites. Any information disclosed depends on how the customers have customized the block pages.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39741	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 296010.	4.3	More Details
CVE-2024-37939	Cross-Site Request Forgery (CSRF) vulnerability in VolThemes Patricia Lite.This issue affects Patricia Lite: from n/a through 1.2.3.	4.3	More Details
CVE-2024-21134	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	4.3	More Details
CVE-2024-6746	A vulnerability classified as problematic was found in NaiboWang EasySpider 0.6.2 on Windows. Affected by this vulnerability is an unknown functionality of the file \EasySpider\resources\app\server.js of the component HTTP GET Request Handler. The manipulation with the input /../../../../../../../../../Windows/win.ini leads to path traversal: '../filedir'. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. The identifier VDB-271477 was assigned to this vulnerability. NOTE: The code maintainer explains, that this is not a big issue "because the default is that the software runs locally without going through the Internet".	4.3	More Details
CVE-2024-37147	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated user can attach a document to any item, even if the user has no write access on it. Upgrade to 10.0.16.	4.3	More Details
CVE-2024-37938	Cross-Site Request Forgery (CSRF) vulnerability in MyThemeShop SociallyViral.This issue affects SociallyViral: from n/a through 1.0.10.	4.3	More Details
CVE-2024-21154	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Human Resources). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2024-39330	An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. Derived classes of the django.core.files.storage.Storage base class, when they override generate_filename() without replicating the file-path validations from the parent class, potentially allow directory traversal via certain inputs during a save() call. (Built-in Storage sub-classes are unaffected.)	4.3	More Details
CVE-2024-1375	The Event post plugin for WordPress is vulnerable to unauthorized bulk metadata update due to a missing nonce check on the save_bulkdatas function in all versions up to, and including, 5.9.5. This makes it possible for unauthenticated attackers to update post_meta_data via a forged request, granted they can trick a logged-in user into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-37941	Cross-Site Request Forgery (CSRF) vulnerability in Internal Link Juicer Internal Link Juicer: SEO Auto Linker for WordPress.This issue affects Internal Link Juicer: SEO Auto Linker for WordPress: from n/a through 2.24.3.	4.3	More Details
CVE-2024-37544	Missing Authorization vulnerability in Tobias Conrad Get Better Reviews for WooCommerce.This issue affects Get Better Reviews for WooCommerce: from n/a through 4.0.6.	4.3	More Details
CVE-2024-6649	A vulnerability has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this vulnerability is the function save_users of the file Users.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271057 was assigned to this vulnerability.	4.3	More Details
CVE-2024-39918	@jmondi/url-to-png is an open source URL to PNG utility featuring parallel rendering using Playwright for screenshots and with storage caching via Local, S3, or CouchDB. Input of the `ImageId` in the code is not sanitized and may lead to path traversal. This allows an attacker to store an image in an arbitrary location that the server has permission to access. This issue has been addressed in version 2.1.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39740	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 displays version information in HTTP requests that could allow an attacker to gather information for future attacks against the system. IBM X-Force ID: 296009.	4.3	More Details
CVE-2024-40630	OpenImageIO is a toolset for reading, writing, and manipulating image files of any image file format relevant to VFX / animation via a format-agnostic API with a feature set, scalability, and robustness needed for feature film production. In affected versions there is a bug in the heif input functionality of OpenImageIO. Specifically, in `HeifInput::seek_subimage()`. In the worst case, this can lead to an information disclosure vulnerability, particularly for programs that directly use the `ImageInput` APIs. This bug has been addressed in commit `0a2dcb4c` which is included in the 2.5.13.1 release. Users are advised to upgrade. There are no known workarounds for this issue.	4.3	More Details
CVE-2024-39729	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 could allow an authenticated user to obtain sensitive information from source code that could be used in further attacks against the system. IBM X-Force ID: 295968.	4.3	More Details
CVE-2024-39908	REXML is an XML toolkit for Ruby. The REXML gem before 3.3.1 has some DoS vulnerabilities when it parses an XML that has many specific characters such as `<`, `0` and `%>`. If you need to parse untrusted XMLs, you many be impacted to these vulnerabilities. The REXML gem 3.3.2 or later include the patches to fix these vulnerabilities. Users are advised to upgrade. Users unable to upgrade should avoid parsing untrusted XML strings.	4.3	More Details
CVE-2024-6410	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.8.9 via the 'pm_upload_image' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the profile picture of any user.	4.3	More Details
CVE-2024-39734	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 296001.	4.3	More Details
CVE-2024-6465	The WP Links Page plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wplf_ajax_update_screenshots' function in all versions up to, and including, 4.9.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to regenerate the link's thumbnail image.	4.3	More Details
CVE-2024-5677	The Featured Image Generator plugin for WordPress is vulnerable to unauthorized image upload due to a missing capability check on the fig_save_after_generate_image function in all versions up to, and including, 1.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary images to a post-related gallery.	4.3	More Details
CVE-2024-5852	The WordPress File Upload plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.24.7 via the 'uploadpath' parameter of the wordpress_file_upload shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload limited files to arbitrary locations on the web server.	4.3	More Details
CVE-2024-6621	The RSS Aggregator – RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wprss_activate_feed_source' and 'wprss_pause_feed_source' functions in all versions up to, and including, 4.23.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate or pause existing RSS feeds.	4.3	More Details
CVE-2024-6579	The Web and WooCommerce Addons for WPBakery Builder plugin for WordPress is vulnerable to unauthorized plugin settings modification due to a missing capability check on several plugin functions in all versions up to, and including, 1.4.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change some of the plugin settings.	4.3	More Details
CVE-2024-39887	An SQL Injection vulnerability in Apache Superset exists due to improper neutralization of special elements used in SQL commands. Specifically, certain engine-specific functions are not checked, which allows attackers to bypass Apache Superset's SQL authorization. To mitigate this, a new configuration key named DISALLOWED_SQL_FUNCTIONS has been introduced. This key disallows the use of the following PostgreSQL functions: version, query_to_xml, inet_server_addr, and inet_client_addr. Additional functions can be added to this list for increased protection. This issue affects Apache Superset: before 4.0.2. Users are recommended to upgrade to version 4.0.2, which fixes the issue.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40637	dbt enables data analysts and engineers to transform their data using the same practices that software engineers use to build applications. When a user installs a package in dbt, it has the ability to override macros, materializations, and other core components of dbt. This is by design, as it allows packages to extend and customize dbt's functionality. However, this also means that a malicious package could potentially override these components with harmful code. This issue has been fixed in versions 1.8.0, 1.6.14 and 1.7.14. Users are advised to upgrade. There are no kn own workarounds for this vulnerability. Users updating to either 1.6.14 or 1.7.14 will need to set `flags.require_explicit_package_overrides_for_builtin_materializations: False` in their configuration in `dbt_project.yml`.	4.2	More Details
CVE-2024-39767	Mattermost Mobile Apps versions <=2.16.0 fail to validate that the push notifications received for a server actually came from this serve that which allows a malicious server to send push notifications with another server's diagnostic ID or server URL and have them show up in mobile apps as that server's push notifications.	4.2	More Details
CVE-2024-37386	An issue was discovered in Stormshield Network Security (SNS) 4.0.0 through 4.3.25, 4.4.0 through 4.7.5, and 4.8.0. Certain manipulations allow restarting in single-user mode despite the activation of secure boot. The following versions fix this: 4.3.27, 4.7.6, and 4.8.2.	4.2	More Details
CVE-2024-31946	An issue was discovered in Stormshield Network Security (SNS) 3.7.0 through 3.7.41, 3.10.0 through 3.11.29, 4.0 through 4.3.24, and 4.4.0 through 4.7.4. A user who has access to the SNS with write access on the email alerts page has the ability to create alert email containing malicious JavaScript, executed by the template preview. The following versions fix this: 3.7.42, 3.11.30, 4.3.25, and 4.7.5.	4.2	More Details
CVE-2024-39732	IBM Datacap Navigator 9.1.5, 9.1.6, 9.1.7, 9.1.8, and 9.1.9 temporarily stores data from different environments that could be obtained by a malicious user. IBM X-Force ID: 295791.	4.1	More Details
CVE-2024-21180	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: OpenSearch Dashboards). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N).	4.1	More Details
CVE-2022-35640	IBM Sterling Partner Engagement Manager 6.2.2 could allow a local attacker to obtain sensitive information when a detailed technical error message is returned. IBM X-Force ID: 230933.	4.0	More Details
CVE-2024-5470	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Guest user with `admin_push_rules` permission may have been able to create project-level deploy tokens.	3.8	More Details
CVE-2024-21144	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2024-21131	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40632	Linkerd is an open source, ultralight, security-first service mesh for Kubernetes. In affected versions when the application being run by linkerd is susceptible to SSRF, an attacker could potentially trigger a denial-of-service (DoS) attack by making requests to localhost:4191/shutdown. Linkerd could introduce an optional environment variable to control a token that must be passed as a header. Linkerd should reject shutdown requests that do not include this header. This issue has been addressed in release version edge-24.6.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	3.7	More Details
CVE-2024-39886	TONE store App version 3.4.2 and earlier contains an issue with unprotected primary channel. Since TONE store App communicates with TONE store website in cleartext, a man-in-the-middle attack may allow an attacker to obtain and/or alter communications of the affected App.	3.7	More Details
CVE-2024-21138	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2024-41007	In the Linux kernel, the following vulnerability has been resolved: tcp: avoid too many retransmit packets If a TCP socket is using TCP_USER_TIMEOUT, and the other peer retracted its window to zero, tcp_retransmit_timer() can retransmit a packet every two jiffies (2 ms for HZ=1000), for about 4 minutes after TCP_USER_TIMEOUT has 'expired'. The fix is to make sure tcp_rtx_probe0_timed_out() takes icsk->icsk_user_timeout into account. Before blamed commit, the socket would not timeout after icsk->icsk_user_timeout, but would use standard exponential backoff for the retransmits. Also worth noting that before commit e89688e3e978 ("net: tcp: fix unexcepted socket die when snd_wnd is 0"), the issue would last 2 minutes instead of 4.	3.3	More Details
CVE-2024-23194	Improper output Neutralization for Logs (CWE-117) in the Command Centre API Diagnostics Endpoint could allow an attacker limited ability to modify Command Centre log files. This issue affects: Gallagher Command Centre v9.10 prior to vEL9.10.1268 (MR1).	3.3	More Details
CVE-2022-48852	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: hdmi: Unregister codec device on unbind On bind we will register the HDMI codec device but we don't unregister it on unbind, leading to a device leakage. Unregister our device at unbind.	3.3	More Details
CVE-2024-6780	Improper permission control in the mobile application (com.android.server.telecom) may lead to user information security risks.	3.3	More Details
CVE-2024-21151	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	3.3	More Details
CVE-2024-21174	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.23, 21.3-21.14 and 23.4. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java VM. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).	3.1	More Details
CVE-2023-41093	Use After Free vulnerability in Silicon Labs Bluetooth SDK on 32 bit, ARM may allow an attacker with precise timing capabilities to intercept a small number of packets intended for a recipient that has left the network.This issue affects Silabs Bluetooth SDK: through 8.0.0.	3.1	More Details
CVE-2024-36452	Cross-site request forgery vulnerability exists in ajaxterm module of Webmin versions prior to 2.003. If this vulnerability is exploited, unintended operations may be performed when a user views a malicious page while logged in. As a result, data within a system may be referred, a webpage may be altered, or a server may be permanently halted.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39919	@jmondi/url-to-png is an open source URL to PNG utility featuring parallel rendering using Playwright for screenshots and with storage caching via Local, S3, or CouchDB. The package includes an `ALLOW_LIST` where the host can specify which services the user is permitted to capture screenshots of. By default, capturing screenshots of web services running on localhost, 127.0.0.1, or the [::] is allowed. If someone hosts this project on a server, users could then capture screenshots of other web services running locally. This issue has been addressed in version 2.1.1 with the addition of a blocklist. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.1	More Details
CVE-2024-40455	An arbitrary file deletion vulnerability in ThinkSAAS v3.7 allows attackers to delete arbitrary files via a crafted request.	2.7	More Details
CVE-2024-2880	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.5 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 in which a user with `admin_group_member` custom role permission could ban group members.	2.7	More Details
CVE-2024-32945	Mattermost Mobile Apps versions <=2.16.0 fail to protect against abuse of a globally shared MathJax state which allows an attacker to change the contents of a LateX post, by creating another post with specific macro definitions.	2.6	More Details
CVE-2024-21164	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:L/I:N/A:N).	2.5	More Details
CVE-2024-6650	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this issue is the function save_designation of the file /classes/Master.php. 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. VDB-271058 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2024-21123	Vulnerability in the Oracle Database Core component of Oracle Database Server. Supported versions that are affected are 19.3-19.23. Easily exploitable vulnerability allows high privileged attacker having SYSDBA privilege with logon to the infrastructure where Oracle Database Core executes to compromise Oracle Database Core. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Core accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	2.3	More Details
CVE-2024-40946	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-40945	In the Linux kernel, the following vulnerability has been resolved: iommu: Return right value in iommu_sva_bind_device() iommu_sva_bind_device() should return either a sva bond handle or an ERR_PTR value in error cases. Existing drivers (idxd and uacce) only check the return value with IS_ERR(). This could potentially lead to a kernel NULL pointer dereference issue if the function returns NULL instead of an error pointer. In reality, this doesn't cause any problems because iommu_sva_bind_device() only returns NULL when the kernel is not configured with CONFIG_IOMMU_SVA. In this case, iommu_dev_enable_feature(dev, IOMMU_DEV_FEAT_SVA) will return an error, and the device drivers won't call iommu_sva_bind_device() at all.	N/A	More Details
CVE-2024-40993	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: Fix suspicious rcu_dereference_protected() When destroying all sets, we are either in pernet exit phase or are executing a "destroy all sets command" from userspace. The latter was taken into account in ip_set_dereference() (nfnetlink mutex is held), but the former was not. The patch adds the required check to rcu_dereference_protected() in ip_set_dereference().	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40947	In the Linux kernel, the following vulnerability has been resolved: ima: Avoid blocking in RCU read-side critical section A panic happens in ima_match_policy: BUG: unable to handle kernel NULL pointer dereference at 0000000000000010 PGD 42f873067 P4D 0 Oops: 0000 [#1] SMP NOPTI CPU: 5 PID: 1286325 Comm: kubeletmonit.sh Kdump: loaded Tainted: P Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 0.0.0 02/06/2015 RIP: 0010:ima_match_policy+0x84/0x450 Code: 49 89 fc 41 89 cf 31 ed 89 44 24 14 eb 1c 44 39 7b 18 74 26 41 83 ff 05 74 20 48 8b 1b 48 3b 1d f2 b9 f4 00 0f 84 9c 01 00 00 <44> 85 73 10 74 ea 44 8b 6b 14 41 f6 c5 01 75 d4 41 f6 c5 02 74 0f RSP: 0018:ff71570009e07a80 EFLAGS: 00010207 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000200 RDX: ffffffffad8dc7c0 RSI: 0000000024924925 RDI: ff3e27850dea2000 RBP: 0000000000000000 R08: 0000000000000000 R09: ffffffffabfce739 R10: ff3e27810cc42400 R11: 0000000000000000 R12: ff3e2781825ef970 R13: 00000000ff3e2785 R14: 000000000000000c R15: 0000000000000001 FS: 00007f5195b51740(0000) GS:ff3e278b12d40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000010 CR3: 0000000626d24002 CR4: 0000000000361ee0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: ima_get_action+0x22/0x30 process_measurement+0xb0/0x830 ? page_add_file_rmap+0x15/0x170 ? alloc_set_pte+0x269/0x4c0 ? prep_new_page+0x81/0x140 ? simple_xattr_get+0x75/0xa0 ? selinux_file_open+0x9d/0xf0 ima_file_check+0x64/0x90 path_openat+0x571/0x1720 do_filp_open+0x9b/0x110 ? page_counter_try_charge+0x57/0xc0 ? files_cgroup_alloc_fd+0x38/0x60 ? __alloc_fd+0xd4/0x250 ? do_sys_open+0x1bd/0x250 do_sys_open+0x1bd/0x250 do_syscall_64+0x5d/0x1d0 entry_SYSCALL_64_after_hwframe+0x65/0xca Commit c7423dbdbc9e ("ima: Handle -ESTALE returned by ima_filter_rule_match()") introduced call to ima_lsm_copy_rule within a RCU read-side critical section which contains kmalloc with GFP_KERNEL. This implies a possible sleep and violates limitations of RCU read-side critical sections on non-PREEMPT systems. Sleeping within RCU read-side critical section might cause synchronize_rcu() returning early and break RCU protection, allowing a UAF to happen. The root cause of this issue could be described as follows: l Thread A l Thread B l l lima_match_policy l l l rcu_read_lock l lima_lsm_update_rule l l l synchronize_rcu l l l l kmalloc(GFP_KERNEL)l l l sleep l ==> synchronize_rcu returns early l kfree(entry) l l l l entry = entry->nextl ==> UAF happens and entry now becomes NULL (or could be anything). l l entry->action l ==> Accessing entry might cause panic. To fix this issue, we are converting all kmalloc that is called within RCU read-side critical section to use GFP_ATOMIC. [PM: fixed missing comment, long lines, !CONFIG_IMA_LSM_RULES case]	N/A	More Details
CVE-2024-6036	A vulnerability in gaizhenbiao/chuanhuchatgpt version 20240410 allows any user to restart the server at will by sending a specific request to the `/queue/join?` endpoint with `"fn_index":66`. This unrestricted server restart capability can severely disrupt service availability, cause data loss or corruption, and potentially compromise system integrity.	N/A	More Details
CVE-2024-40992	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix responder length checking for UD request packets According to the IBA specification: If a UD request packet is detected with an invalid length, the request shall be an invalid request and it shall be silently dropped by the responder. The responder then waits for a new request packet. commit 689c5421bfe0 ("RDMA/rxe: Fix incorrect responder length checking") defers responder length check for UD QPs in function `copy_data`. But it introduces a regression issue for UD QPs. When the packet size is too large to fit in the receive buffer. `copy_data` will return error code -EINVAL. Then `send_data_in` will return RESPST_ERR_MALFORMED_WQE. UD QP will transfer into ERROR state.	N/A	More Details
CVE-2024-40991	In the Linux kernel, the following vulnerability has been resolved: dmaengine: ti: k3-udma-glue: Fix of_k3_udma_glue_parse_chn_by_id() The of_k3_udma_glue_parse_chn_by_id() helper function erroneously invokes "of_node_put()" on the "udmax_np" device-node passed to it, without having incremented its reference count at any point. Fix it.	N/A	More Details
CVE-2024-40990	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Add check for srq max_sge attribute max_sge attribute is passed by the user, and is inserted and used unchecked, so verify that the value doesn't exceed maximum allowed value before using it.	N/A	More Details
CVE-2024-40948	In the Linux kernel, the following vulnerability has been resolved: mm/page_table_check: fix crash on ZONE_DEVICE Not all pages may apply to pgtable check. One example is ZONE_DEVICE pages: they map PFNs directly, and they don't allocate page_ext at all even if there's struct page around. One may reference devm_memremap_pages(). When both ZONE_DEVICE and page-table-check enabled, then try to map some dax memories, one can trigger kernel bug constantly now when the kernel was trying to inject some pfn maps on the dax device: kernel BUG at mm/page_table_check.c:55! While it's pretty legal to use set_pxx_at() for ZONE_DEVICE pages for page fault resolutions, skip all the checks if page_ext doesn't even exist in pgtable checker, which applies to ZONE_DEVICE but maybe more.	N/A	More Details
CVE-2024-6630	Rejected reason: **REJECT** This CVE ID was issued in error and is a duplicate. Please use CVE-2024-6500 instead.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40949	In the Linux kernel, the following vulnerability has been resolved: mm: shmem: fix getting incorrect lruvec when replacing a shmem folio When testing shmem swapin, I encountered the warning below on my machine. The reason is that replacing an old shmem folio with a new one causes mem_cgroup_migrate() to clear the old folio's memcg data. As a result, the old folio cannot get the correct memcg's lruvec needed to remove itself from the LRU list when it is being freed. This could lead to possible serious problems, such as LRU list crashes due to holding the wrong LRU lock, and incorrect LRU statistics. To fix this issue, we can fallback to use the mem_cgroup_replace_folio() to replace the old shmem folio. [5241.100311] page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x5d9960 [5241.100317] head: order:4 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0 [5241.100319] flags: 0x17fffe0000040068(uptodatelrulheadlswapbackedlnode=0lzone=2llastcpupid=0x3ffff) [5241.100323] raw: 17fffe0000040068 ffffffdffd6687948 ffffffdffd69ae008 0000000000000000 [5241.100325] raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 [5241.100326] head: 17fffe0000040068 ffffffdffd6687948 ffffffdffd69ae008 0000000000000000 [5241.100327] head: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 [5241.100328] head: 17fffe0000000204 ffffffdffd6665801 ffffffffffffffff 0000000000000000 [5241.100329] head: 0000000a00000010 0000000000000000 00000000ffffffff 0000000000000000 [5241.100330] page dumped because: VM_WARN_ON_ONCE_FOLIO(!memcg && !mem_cgroup_disabled()) [5241.100338] ------------[cut here]------------ [5241.100339] WARNING: CPU: 19 PID: 78402 at include/linux/memcontrol.h:775 folio_lruvec_lock_irqsave+0x140/0x150 [...] [5241.100374] pc : folio_lruvec_lock_irqsave+0x140/0x150 [5241.100375] lr : folio_lruvec_lock_irqsave+0x138/0x150 [5241.100376] sp : ffff80008b38b930 [...] [5241.100398] Call trace: [5241.100399] folio_lruvec_lock_irqsave+0x140/0x150 [5241.100401] __page_cache_release+0x90/0x300 [5241.100404] __folio_put+0x50/0x108 [5241.100406] shmem_replace_folio+0x1b4/0x240 [5241.100409] shmem_swapin_folio+0x314/0x528 [5241.100411] shmem_get_folio_gfp+0x3b4/0x930 [5241.100412] shmem_fault+0x74/0x160 [5241.100414] __do_fault+0x40/0x218 [5241.100417] do_shared_fault+0x34/0x1b0 [5241.100419] do_fault+0x40/0x168 [5241.100420] handle_pte_fault+0x80/0x228 [5241.100422] __handle_mm_fault+0x1c4/0x440 [5241.100424] handle_mm_fault+0x60/0x1f0 [5241.100426] do_page_fault+0x120/0x488 [5241.100429] do_translation_fault+0x4c/0x68 [5241.100431] do_mem_abort+0x48/0xa0 [5241.100434] el0_da+0x38/0xc0 [5241.100436] el0t_64_sync_handler+0x68/0xc0 [5241.100437] el0t_64_sync+0x14c/0x150 [5241.100439] ---[end trace 0000000000000000]--- [baolin.wang@linux.alibaba.com: remove less helpful comments, per Matthew] Link: https://lkml.kernel.org/r/ccad3fe1375b468ebca3227b6b729f3eaf9d8046.1718423197.git.baolin.wang@linux.alibaba.com	N/A	More Details
CVE-2024-40944	In the Linux kernel, the following vulnerability has been resolved: x86/kexec: Fix bug with call depth tracking The call to cc_platform_has() triggers a fault and system crash if call depth tracking is active because the GS segment has been reset by load_segments() and GS_BASE is now 0 but call depth tracking uses per-CPU variables to operate. Call cc_platform_has() earlier in the function when GS is still valid. [bp: Massage.]	N/A	More Details
CVE-2024-6037	A vulnerability in gaizhenbiao/chuanhuchatgpt version 20240410 allows an attacker to create arbitrary folders at any location on the server, including the root directory (C: dir). This can lead to uncontrolled resource consumption, resulting in resource exhaustion, denial of service (DoS), server unavailability, and potential data loss or corruption.	N/A	More Details
CVE-2024-40943	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix races between hole punching and AIO+DIO After commit "ocfs2: return real error code in ocfs2_dio_wr_get_block", fstests/generic/300 become from always failed to sometimes failed: ========== [473.293420] run fstests generic/300 [475.296983] JBD2: Ignoring recovery information on journal [475.302473] ocfs2: Mounting device (253,1) on (node local, slot 0) with ordered data mode. [494.290998] OCFS2: ERROR (device dm-1): ocfs2_change_extent_flag: Owner 5668 has an extent at cpos 78723 which can no longer be found [494.291609] On-disk corruption discovered. Please run fsck.ocfs2 once the filesystem is unmounted. [494.292018] OCFS2: File system is now read-only. [494.292224] (kworker/19:11,2628,19):ocfs2_mark_extent_written:5272 ERROR: status = -30 [494.292602] (kworker/19:11,2628,19):ocfs2_dio_end_io_write:2374 ERROR: status = -3 fio: io_u error on file /mnt/scratch/racer: Read-only file system: write offset=460849152, buflen=131072 ========== In __blockdev_direct_IO, ocfs2_dio_wr_get_block is called to add unwritten extents to a list. extents are also inserted into extent tree in ocfs2_write_begin_nolock. Then another thread call fallocate to puch a hole at one of the unwritten extent. The extent at cpos was removed by ocfs2_remove_extent(). At end io worker thread, ocfs2_search_extent_list found there is no such extent at the cpos. T1 T2 T3 inode lock ... insert extents ... inode unlock ocfs2_fallocate __ocfs2_change_file_space inode lock lock ip_alloc_sem ocfs2_remove_inode_range inode ocfs2_remove_btree_range ocfs2_remove_extent ^---remove the extent at cpos 78723 ... unlock ip_alloc_sem inode unlock ocfs2_dio_end_io ocfs2_dio_end_io_write lock ip_alloc_sem ocfs2_mark_extent_written ocfs2_change_extent_flag ocfs2_search_extent_list ^---failed to find extent ... unlock ip_alloc_sem In most filesystems, fallocate is not compatible with racing with AIO+DIO, so fix it by adding to wait for all dio before fallocate/punch_hole like ext4.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41005	In the Linux kernel, the following vulnerability has been resolved: netpoll: Fix race condition in netpoll_owner_active KCSAN detected a race condition in netpoll: BUG: KCSAN: data-race in net_rx_action / netpoll_send_skb write (marked) to 0xffff8881164168b0 of 4 bytes by interrupt on cpu 10: net_rx_action (./include/linux/netpoll.h:90 net/core/dev.c:6712 net/core/dev.c:6822) <snip> read to 0xffff8881164168b0 of 4 bytes by task 1 on cpu 2: netpoll_send_skb (net/core/netpoll.c:319 net/core/netpoll.c:345 net/core/netpoll.c:393) netpoll_send_udp (net/core/netpoll.c:?) <snip> value changed: 0x0000000a -> 0xffffffff This happens because netpoll_owner_active() needs to check if the current CPU is the owner of the lock, touching napi->poll_owner non atomically. The ->poll_owner field contains the current CPU holding the lock. Use an atomic read to check if the poll owner is the current CPU.	N/A	More Details
CVE-2024-40950	In the Linux kernel, the following vulnerability has been resolved: mm: huge_memory: fix misused mapping_large_folio_support() for anon folios When I did a large folios split test, a WARNING "[5059.122759][T166] Cannot split file folio to non-0 order" was triggered. But the test cases are only for anonmous folios. while mapping_large_folio_support() is only reasonable for page cache folios. In split_huge_page_to_list_to_order(), the folio passed to mapping_large_folio_support() maybe anonmous folio. The folio_test_anon() check is missing. So the split of the anonmous THP is failed. This is also the same for shmem_mapping(). We'd better add a check for both. But the shmem_mapping() in __split_huge_page() is not involved, as for anonmous folios, the end parameter is set to -1, so (head[i].index >= end) is always false. shmem_mapping() is not called. Also add a VM_WARN_ON_ONCE() in mapping_large_folio_support() for anon mapping, So we can detect the wrong use more easily. THP folios maybe exist in the pagecache even the file system doesn't support large folio, it is because when CONFIG_TRANSPARENT_HUGEPAGE is enabled, khugepaged will try to collapse read-only file-backed pages to THP. But the mapping does not actually support multi order large folios properly. Using /sys/kernel/debug/split_huge_pages to verify this, with this patch, large anon THP is successfully split and the warning is ceased.	N/A	More Details
CVE-2024-32759	Under certain circumstances the Software House C●CURE 9000 installer will utilize weak credentials.	N/A	More Details
CVE-2024-41004	In the Linux kernel, the following vulnerability has been resolved: tracing: Build event generation tests only as modules The kprobes and synth event generation test modules add events and lock (get a reference) those event file reference in module init function, and unlock and delete it in module exit function. This is because those are designed for playing as modules. If we make those modules as built-in, those events are left locked in the kernel, and never be removed. This causes kprobe event self-test failure as below. [97.349708] ------------[cut here]------------ [97.353453] WARNING: CPU: 3 PID: 1 at kernel/trace/trace_kprobe.c:2133 kprobe_trace_self_tests_init+0x3f1/0x480 [97.357106] Modules linked in: [97.358488] CPU: 3 PID: 1 Comm: swapper/0 Not tainted 6.9.0-g699646734ab5-dirty #14 [97.361556] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 [97.363880] RIP: 0010:kprobe_trace_self_tests_init+0x3f1/0x480 [97.365538] Code: a8 24 08 82 e9 ae fd ff ff 90 0f 0b 90 48 c7 c7 e5 aa 0b 82 e9 ee fc ff ff 90 0f 0b 90 48 c7 c7 2d 61 06 82 e9 8e fd ff ff 90 <0f> 0b 90 48 c7 c7 33 0b 0c 82 89 c6 e8 6e 03 1f ff 41 ff c7 e9 90 [97.370429] RSP: 0000:ffffc90000013b50 EFLAGS: 00010286 [97.371852] RAX: 00000000ffffffff0 RBX: ffff888005919c00 RCX: 0000000000000000 [97.373829] RDX: ffff888003f40000 RSI: ffffffff8236a598 RDI: ffff888003f40a68 [97.375715] RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 [97.377675] R10: ffffffff811c9ae5 R11: ffffffff8120c4e0 R12: 0000000000000000 [97.379591] R13: 0000000000000001 R14: 0000000000000015 R15: 0000000000000000 [97.381536] FS: 0000000000000000(0000) GS:ffff88807dcc0000(0000) knlGS:0000000000000000 [97.383813] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [97.385449] CR2: 0000000000000000 CR3: 0000000002244000 CR4: 00000000000006b0 [97.387347] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [97.389277] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [97.391196] Call Trace: [97.391967] <TASK> [97.392647] ? __warn+0xcc/0x180 [97.393640] ? kprobe_trace_self_tests_init+0x3f1/0x480 [97.395181] ? report_bug+0xbd/0x150 [97.396234] ? handle_bug+0x3e/0x60 [97.397311] ? exc_invalid_op+0x1a/0x50 [97.398434] ? asm_exc_invalid_op+0x1a/0x20 [97.399652] ? trace_kprobe_is_busy+0x20/0x20 [97.400904] ? tracing_reset_all_online_cpus+0x15/0x90 [97.402304] ? kprobe_trace_self_tests_init+0x3f1/0x480 [97.403773] ? init_kprobe_trace+0x50/0x50 [97.404972] do_one_initcall+0x112/0x240 [97.406113] do_initcall_level+0x95/0xb0 [97.407286] ? kernel_init+0x1a/0x1a0 [97.408401] do_initcalls+0x3f/0x70 [97.409452] kernel_init_freeable+0x16f/0x1e0 [97.410662] ? rest_init+0x1f0/0x1f0 [97.411738] kernel_init+0x1a/0x1a0 [97.412788] ret_from_fork+0x39/0x50 [97.413817] ? rest_init+0x1f0/0x1f0 [97.414844] ret_from_fork_asm+0x11/0x20 [97.416285] </TASK> [97.417134] irq event stamp: 13437323 [97.418376] hardirqs last enabled at (13437337): [<ffffffff8110bc0c>] console_unlock+0x11c/0x150 [97.421285] hardirqs last disabled at (13437370): [<ffffffff8110bbf1>] console_unlock+0x101/0x150 [97.423838] softirqs last enabled at (13437366): [<ffffffff8108e17f>] handle_softirqs+0x23f/0x2a0 [97.426450] softirqs last disabled at (13437393): [<ffffffff8108e346>] __irq_exit_rcu+0x66/0xd0 [97.428850] ---[end trace 0000000000000000]--- And also, since we can not cleanup dynamic_event file, ftracetest are failed too. To avoid these issues, build these tests only as modules.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22018	A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-read flag is used. This flaw arises from an inadequate permission model that fails to restrict file stats through the fs.lstat API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 21. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	N/A	More Details
CVE-2024-40942	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: mesh: Fix leak of mesh_preq_queue objects The hwmp code use objects of type mesh_preq_queue, added to a list in ieee80211_if_mesh, to keep track of mpath we need to resolve. If the mpath gets deleted, ex mesh interface is removed, the entries in that list will never get cleaned. Fix this by flushing all corresponding items of the preq_queue in mesh_path_flush_pending(). This should take care of KASAN reports like this: unreferenced object 0xffff00000668d800 (size 128): comm "kworker/u8:4", pid 67, jiffies 4295419552 (age 1836.444s) hex dump (first 32 bytes): 00 1f 05 09 00 00 ff ff 00 d5 68 06 00 00 ff ff .....h..... 8e 97 ea eb 3e b8 01 00 00 00 00 00 00 00 00 00 ....>..... backtrace: [<000000007302a0b6>] __kmem_cache_alloc_node+0x1e0/0x35c [<00000000049bd418>] kmalloc_trace+0x34/0x80 [<0000000000d792bb>] mesh_queue_preq+0x44/0x2a8 [<00000000c99c3696>] mesh_nexthop_resolve+0x198/0x19c [<00000000926bf598>] ieee80211_xmit+0x1d0/0x1f4 [<00000000fc8c2284>] __ieee80211_subif_start_xmit+0x30c/0x764 [<000000005926ee38>] ieee80211_subif_start_xmit+0x9c/0x7a4 [<000000004c86e916>] dev_hard_start_xmit+0x174/0x440 [<0000000023495647>] __dev_queue_xmit+0xe24/0x111c [<00000000cfe9ca78>] batadv_send_skb_packet+0x180/0x1e4 [<000000007bacc5d5>] batadv_v_elp_periodic_work+0x2f4/0x508 [<00000000adc3cd94>] process_one_work+0x4b8/0xa1c [<00000000b36425d1>] worker_thread+0x9c/0x634 [<0000000005852dd5>] kthread+0x1bc/0x1c4 [<000000005fccd770>] ret_from_fork+0x10/0x20 unreferenced object 0xffff000009051f00 (size 128): comm "kworker/u8:4", pid 67, jiffies 4295419553 (age 1836.440s) hex dump (first 32 bytes): 90 d6 92 0d 00 00 ff ff 00 d8 68 06 00 00 ff ff .....h..... 36 27 92 e4 02 e0 01 00 00 58 79 06 00 00 ff ff 6'.....Xy..... backtrace: [<000000007302a0b6>] __kmem_cache_alloc_node+0x1e0/0x35c [<00000000049bd418>] kmalloc_trace+0x34/0x80 [<0000000000d792bb>] mesh_queue_preq+0x44/0x2a8 [<00000000c99c3696>] mesh_nexthop_resolve+0x198/0x19c [<00000000926bf598>] ieee80211_xmit+0x1d0/0x1f4 [<00000000fc8c2284>] __ieee80211_subif_start_xmit+0x30c/0x764 [<000000005926ee38>] ieee80211_subif_start_xmit+0x9c/0x7a4 [<000000004c86e916>] dev_hard_start_xmit+0x174/0x440 [<0000000023495647>] __dev_queue_xmit+0xe24/0x111c [<00000000cfe9ca78>] batadv_send_skb_packet+0x180/0x1e4 [<000000007bacc5d5>] batadv_v_elp_periodic_work+0x2f4/0x508 [<00000000adc3cd94>] process_one_work+0x4b8/0xa1c [<00000000b36425d1>] worker_thread+0x9c/0x634 [<0000000005852dd5>] kthread+0x1bc/0x1c4 [<000000005fccd770>] ret_from_fork+0x10/0x20	N/A	More Details
CVE-2024-3325	Vulnerability in Jaspersoft JasperReport Servers.This issue affects JasperReport Servers: from 8.0.4 through 9.0.0.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41003	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix reg_set_min_max corruption of fake_reg Juan reported that after doing some changes to buzzer [0] and implementing a new fuzzing strategy guided by coverage, they noticed the following in one of the probes: [...] 13: (79) r6 = *(u64 *)(r0 +0) ; R0=map_value(ks=4,vs=8) R6_w=scalar() 14: (b7) r0 = 0 ; R0_w=0 15: (b4) w0 = -1 ; R0_w=0xffffffff 16: (74) w0 >>= 1 ; R0_w=0x7fffffff 17: (5c) w6 &= w0 ; R0_w=0x7fffffff R6_w=scalar(smin=smin32=0,smax=umax=umax32=0x7fffffff,var_off=(0x0; 0x7fffffff)) 18: (44) w6 |= 2 ; R6_w=scalar(smin=umin=smin32=umin32=2,smax=umax=umax32=0x7fffffff,var_off=(0x2; 0x7ffffffd)) 19: (56) if w6 != 0x7ffffffd goto pc+1 REG INVARIANTS VIOLATION (true_reg2): range bounds violation u64=[0x7fffffff, 0x7ffffffd] s64=[0x7fffffff, 0x7ffffffd] u32=[0x7fffffff, 0x7ffffffd] s32=[0x7fffffff, 0x7ffffffd] var_off=(0x7fffffff, 0x0) REG INVARIANTS VIOLATION (false_reg1): range bounds violation u64=[0x7fffffff, 0x7ffffffd] s64=[0x7fffffff, 0x7ffffffd] u32=[0x7fffffff, 0x7ffffffd] s32=[0x7fffffff, 0x7ffffffd] var_off=(0x7fffffff, 0x0) REG INVARIANTS VIOLATION (false_reg2): const tnum out of sync with range bounds u64=[0x0, 0xffffffffffffffff] s64=[0x8000000000000000, 0x7fffffffffffffff] u32=[0x0, 0xffffffff] s32=[0x80000000, 0x7fffffff] var_off=(0x7fffffff, 0x0) 19: R6_w=0x7fffffff 20: (95) exit from 19 to 21: R0=0x7fffffff R6=scalar(smin=umin=smin32=umin32=2,smax=umax=smax32=umax32=0x7ffffffe,var_off=(0x2; 0x7ffffffd)) R7=map_ptr(ks=4,vs=8) R9=ctx() R10=fp0 fp-24=map_ptr(ks=4,vs=8) fp-40=mmmmmmmm 21: R0=0x7fffffff R6=scalar(smin=umin=smin32=umin32=2,smax=umax=smax32=umax32=0x7ffffffe,var_off=(0x2; 0x7ffffffd)) R7=map_ptr(ks=4,vs=8) R9=ctx() R10=fp0 fp-24=map_ptr(ks=4,vs=8) fp-40=mmmmmmmm 21: (14) w6 -= 2147483632 ; R6_w=scalar(smin=umin=umin32=2,smax=umax=0xffffffff,smin32=0x80000012,smax32=14,var_off=(0x2; 0xffffffd)) 22: (76) if w6 s>= 0xe goto pc+1 ; R6_w=scalar(smin=umin=umin32=2,smax=umax=0xffffffff,smin32=0x80000012,smax32=13,var_off=(0x2; 0xffffffd)) 23: (95) exit from 22 to 24: R0=0x7fffffff R6_w=14 R7=map_ptr(ks=4,vs=8) R9=ctx() R10=fp0 fp-24=map_ptr(ks=4,vs=8) fp-40=mmmmmmmm 24: R0=0x7fffffff R6_w=14 R7=map_ptr(ks=4,vs=8) R9=ctx() R10=fp0 fp-24=map_ptr(ks=4,vs=8) fp-40=mmmmmmmm 24: (14) w6 -= 14 ; R6_w=0 [...] What can be seen here is a register invariant violation on line 19. After the binary-or in line 18, the verifier knows that bit 2 is set but knows nothing about the rest of the content which was loaded from a map value, meaning, range is [2,0x7fffffff] with var_off=(0x2; 0x7ffffffd). When in line 19 the verifier analyzes the branch, it splits the register states in reg_set_min_max() into the registers of the true branch (true_reg1, true_reg2) and the registers of the false branch (false_reg1, false_reg2). Since the test is w6 != 0x7ffffffd, the src_reg is a known constant. Internally, the verifier creates a "fake" register initialized as scalar to the value of 0x7ffffffd, and then passes it onto reg_set_min_max(). Now, for line 19, it is mathematically impossible to take the false branch of this program, yet the verifier analyzes it. It is impossible because the second bit of r6 will be set due to the prior or operation and the constant in the condition has that bit unset (hex(fd) == binary(1111 1101). When the verifier first analyzes the false / fall-through branch, it will compute an intersection between the var_off of r6 and of the constant. This is because the verifier creates a "fake" register initialized to the value of the constant. The intersection result later refines both registers in regs_refine_cond_op(): [...] t = tnum_intersect(tnum_subreg(reg1->var_off), tnum_subreg(reg2->var_off)); reg1->var_o ---truncated---	N/A	More Details
CVE-2024-6433	The application zips all the files in the folder specified by the user, which allows an attacker to read arbitrary files on the system by providing a crafted path. This vulnerability can be exploited by sending a request to the application with a malicious snapshot_path parameter.	N/A	More Details
CVE-2024-21687	This High severity File Inclusion vulnerability was introduced in versions 9.0.0, 9.1.0, 9.2.0, 9.3.0, 9.4.0, 9.5.0 and 9.6.0 of Bamboo Data Center and Server. This File Inclusion vulnerability, with a CVSS Score of 8.1, allows an authenticated attacker to get the application to display the contents of a local file, or execute a different files already stored locally on the server which has high impact to confidentiality, high impact to integrity, no impact to availability, and requires no user interaction. Atlassian recommends that Bamboo Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions listed on this CVE See the release notes (https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-1189793869.html). You can download the latest version of Bamboo Data Center and Server from the download center (https://www.atlassian.com/software/bamboo/download-archives). This vulnerability was reported via our Bug Bounty program.	N/A	More Details
CVE-2024-21686	This High severity Stored XSS vulnerability was introduced in versions 7.13 of Confluence Data Center and Server. This Stored XSS vulnerability, with a CVSS Score of 7.3, allows an authenticated attacker to execute arbitrary HTML or JavaScript code on a victims browser which has high impact to confidentiality, high impact to integrity, no impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions listed on this CVE See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). This vulnerability was reported via our Bug Bounty program.	N/A	More Details
CVE-2024-40999	In the Linux kernel, the following vulnerability has been resolved: net: ena: Add validation for completion descriptors consistency Validate that `first` flag is set only for the first descriptor in multi-buffer packets. In case of an invalid descriptor, a reset will occur. A new reset reason for RX data corruption has been added.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32670	Exposure of Sensitive Information to an Unauthorized Actor in Samsung Galaxy SmartTag2 prior to 0.20.04 allows attackes to potentially identify the tag's location by scanning the BLE adversting.	N/A	More Details
CVE-2024-40989	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Disassociate vcpus from redistributor region on teardown When tearing down a redistributor region, make sure we don't have any dangling pointer to that region stored in a vcpu.	N/A	More Details
CVE-2024-40974	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Enforce hcall result buffer validity and size plpar_hcall(), plpar_hcall9(), and related functions expect callers to provide valid result buffers of certain minimum size. Currently this is communicated only through comments in the code and the compiler has no idea. For example, if I write a bug like this: long retbuf[PLPAR_HCALL_BUFSIZE]; // should be PLPAR_HCALL9_BUFSIZE plpar_hcall9(H_ALLOCATE_VAS_WINDOW, retbuf, ...); This compiles with no diagnostics emitted, but likely results in stack corruption at runtime when plpar_hcall9() stores results past the end of the array. (To be clear this is a contrived example and I have not found a real instance yet.) To make this class of error less likely, we can use explicitly-sized array parameters instead of pointers in the declarations for the hcall APIs. When compiled with -Warray-bounds[1], the code above now provokes a diagnostic like this: error: array argument is too small; is of size 32, callee requires at least 72 [-Werror,-Warray-bounds] 60 | plpar_hcall9(H_ALLOCATE_VAS_WINDOW, retbuf, | ^~~~~~ [1] Enabled for LLVM builds but not GCC for now. See commit 0da6e5fd6c37 ("gcc: disable '-Warray-bounds' for gcc-13 too") and related changes.	N/A	More Details
CVE-2024-40988	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: fix UBSAN warning in kv_dpm.c Adds bounds check for sumo_vid_mapping_entry.	N/A	More Details
CVE-2024-6286	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	N/A	More Details
CVE-2024-6150	A non-admin user can cause short-term disruption in Target VM availability in Citrix Provisioning	N/A	More Details
CVE-2024-40972	In the Linux kernel, the following vulnerability has been resolved: ext4: do not create EA inode under buffer lock ext4_xattr_set_entry() creates new EA inodes while holding buffer lock on the external xattr block. This is problematic as it nests all the allocation locking (which acquires locks on other buffers) under the buffer lock. This can even deadlock when the filesystem is corrupted and e.g. quota file is setup to contain xattr block as data block. Move the allocation of EA inode out of ext4_xattr_set_entry() into the callers.	N/A	More Details
CVE-2024-40975	In the Linux kernel, the following vulnerability has been resolved: platform/x86: x86-android-tablets: Unregister devices in reverse order Not all subsystems support a device getting removed while there are still consumers of the device with a reference to the device. One example of this is the regulator subsystem. If a regulator gets unregistered while there are still drivers holding a reference a WARN() at drivers/regulator/core.c:5829 triggers, e.g.: WARNING: CPU: 1 PID: 1587 at drivers/regulator/core.c:5829 regulator_unregister Hardware name: Intel Corp. VALLEYVIEW C0 PLATFORM/BYT-T FFD8, BIOS BLADE_21.X64.0005.R00.1504101516 FFD8_X64_R_2015_04_10_1516 04/10/2015 RIP: 0010:regulator_unregister Call Trace: <TASK> regulator_unregister devres_release_group i2c_device_remove device_release_driver_internal bus_remove_device device_del device_unregister x86_android_tablet_remove On the Lenovo Yoga Tablet 2 series the bq24190 charger chip also provides a 5V boost converter output for powering USB devices connected to the micro USB port, the bq24190-charger driver exports this as a Vbus regulator. On the 830 (8") and 1050 ("10") models this regulator is controlled by a platform_device and x86_android_tablet_remove() removes platform_device-s before i2c_clients so the consumer gets removed first. But on the 1380 (13") model there is a lc824206xa micro-USB switch connected over I2C and the extcon driver for that controls the regulator. The bq24190 i2c-client *must* be registered first, because that creates the regulator with the lc824206xa listed as its consumer. If the regulator has not been registered yet the lc824206xa driver will end up getting a dummy regulator. Since in this case both the regulator provider and consumer are I2C devices, the only way to ensure that the consumer is unregistered first is to unregister the I2C devices in reverse order of in which they were created. For consistency and to avoid similar problems in the future change x86_android_tablet_remove() to unregister all device types in reverse order.	N/A	More Details
CVE-2024-40971	In the Linux kernel, the following vulnerability has been resolved: f2fs: remove clear SB_INLINECRYPT flag in default_options In f2fs_remount, SB_INLINECRYPT flag will be clear and re-set. If create new file or open file during this gap, these files will not use inlinecrypt. Worse case, it may lead to data corruption if wrappedkey_v0 is enable. Thread A: Thread B: -f2fs_remount -f2fs_file_open or f2fs_new_inode -default_options <- clear SB_INLINECRYPT flag -fscrypt_select_encryption_impl -parse_options <- set SB_INLINECRYPT again	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39491	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: cs35l56: Fix lifetime of cs_dsp instance The cs_dsp instance is initialized in the driver probe() so it should be freed in the driver remove(). Also fix a missing call to cs_dsp_remove() in the error path of cs35l56_hda_common_probe(). The call to cs_dsp_remove() was being done in the component unbind callback cs35l56_hda_unbind(). This meant that if the driver was unbound and then re-bound it would be using an uninitialized cs_dsp instance. It is best to initialize the cs_dsp instance in probe() so that it can return an error if it fails. The component binding API doesn't have any error handling so there's no way to handle a failure if cs_dsp was initialized in the bind.	N/A	More Details
CVE-2024-40941	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: don't read past the mfuart notifcation In case the firmware sends a notification that claims it has more data than it has, we will read past that was allocated for the notification. Remove the print of the buffer, we won't see it by default. If needed, we can see the content with tracing. This was reported by KFENCE.	N/A	More Details
CVE-2024-39488	In the Linux kernel, the following vulnerability has been resolved: arm64: asm-bug: Add .align 2 to the end of __BUG_ENTRY When CONFIG_DEBUG_BUGVERBOSE=n, we fail to add necessary padding bytes to bug_table entries, and as a result the last entry in a bug table will be ignored, potentially leading to an unexpected panic(). All prior entries in the table will be handled correctly. The arm64 ABI requires that struct fields of up to 8 bytes are naturally-aligned, with padding added within a struct such that struct are suitably aligned within arrays. When CONFIG_DEBUG_BUGVERPOSE=y, the layout of a bug_entry is: struct bug_entry { signed int bug_addr_disp; // 4 bytes signed int file_disp; // 4 bytes unsigned short line; // 2 bytes unsigned short flags; // 2 bytes } ... with 12 bytes total, requiring 4-byte alignment. When CONFIG_DEBUG_BUGVERBOSE=n, the layout of a bug_entry is: struct bug_entry { signed int bug_addr_disp; // 4 bytes unsigned short flags; // 2 bytes < implicit padding > // 2 bytes } ... with 8 bytes total, with 6 bytes of data and 2 bytes of trailing padding, requiring 4-byte alginment. When we create a bug_entry in assembly, we align the start of the entry to 4 bytes, which implicitly handles padding for any prior entries. However, we do not align the end of the entry, and so when CONFIG_DEBUG_BUGVERBOSE=n, the final entry lacks the trailing padding bytes. For the main kernel image this is not a problem as find_bug() doesn't depend on the trailing padding bytes when searching for entries: for (bug = __start___bug_table; bug < __stop___bug_table; ++bug) if (bugaddr == bug_addr(bug)) return bug; However for modules, module_bug_finalize() depends on the trailing bytes when calculating the number of entries: mod->num_bugs = sechdrs[i].sh_size / sizeof(struct bug_entry); ... and as the last bug_entry lacks the necessary padding bytes, this entry will not be counted, e.g. in the case of a single entry: sechdrs[i].sh_size == 6 sizeof(struct bug_entry) == 8; sechdrs[i].sh_size / sizeof(struct bug_entry) == 0; Consequently module_find_bug() will miss the last bug_entry when it does: for (i = 0; i < mod->num_bugs; ++i, ++bug) if (bugaddr == bug_addr(bug)) goto out; ... which can lead to a kenrel panic due to an unhandled bug. This can be demonstrated with the following module: static int __init buginit(void) { WARN(1, "hello\n"); return 0; } static void __exit bugexit(void) { } module_init(buginit); module_exit(bugexit); MODULE_LICENSE("GPL"); ... which will trigger a kernel panic when loaded: ------------[cut here]------------ hello Unexpected kernel BRK exception at EL1 Internal error: BRK handler: 00000000f2000800 [#1] PREEMPT SMP Modules linked in: hello(O+) CPU: 0 PID: 50 Comm: insmod Tainted: G O 6.9.1 #8 Hardware name: linux,dummy-virt (DT) pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : buginit+0x18/0x1000 [hello] lr : buginit+0x18/0x1000 [hello] sp : ffff800080533ae0 x29: ffff800080533ae0 x28: 0000000000000000 x27: 0000000000000000 x26: ffffaba8c4e70510 x25: ffff800080533c30 x24: ffffaba8c4a28a58 x23: 0000000000000000 x22: 0000000000000000 x21: ffff3947c0eab3c0 x20: ffffaba8c4e3f000 x19: ffffaba846464000 x18: 0000000000000006 x17: 0000000000000000 x16: ffffaba8c2492834 x15: 0720072007200720 x14: 0720072007200720 x13: ffffaba8c49b27c8 x12: 0000000000000312 x11: 0000000000000106 x10: ffffaba8c4a0a7c8 x9 : ffffaba8c49b27c8 x8 : 00000000ffffefff x7 : ffffaba8c4a0a7c8 x6 : 80000000fffff000 x5 : 0000000000000107 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff3947c0eab3c0 Call trace: buginit+0x18/0x1000 [hello] do_one_initcall+0x80/0x1c8 do_init_module+0x60/0x218 load_module+0x1ba4/0x1d70 __do_sys_init_module+0x198/0x1d0 __arm64_sys_init_module+0x1c/0x28 invoke_syscall+0x48/0x114 el0_svc ---truncated---	N/A	More Details
CVE-2024-40968	In the Linux kernel, the following vulnerability has been resolved: MIPS: Octeon: Add PCIe link status check The standard PCIe configuration read-write interface is used to access the configuration space of the peripheral PCIe devices of the mips processor after the PCIe link surprise down, it can generate kernel panic caused by "Data bus error". So it is necessary to add PCIe link status check for system protection. When the PCIe link is down or in training, assigning a value of 0 to the configuration address can prevent read-write behavior to the configuration space of peripheral PCIe devices, thereby preventing kernel panic.	N/A	More Details
CVE-2024-6235	Sensitive information disclosure in NetScaler Console	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40976	In the Linux kernel, the following vulnerability has been resolved: drm/lima: mask irqs in timeout path before hard reset There is a race condition in which a rendering job might take just long enough to trigger the drm sched job timeout handler but also still complete before the hard reset is done by the timeout handler. This runs into race conditions not expected by the timeout handler. In some very specific cases it currently may result in a refcount imbalance on lima_pm_idle, with a stack dump such as: [10136.669170] WARNING: CPU: 0 PID: 0 at drivers/gpu/drm/lima/lima_devfreq.c:205 lima_devfreq_record_idle+0xa0/0xb0 ... [10136.669459] pc : lima_devfreq_record_idle+0xa0/0xb0 ... [10136.669628] Call trace: [10136.669634] lima_devfreq_record_idle+0xa0/0xb0 [10136.669646] lima_sched_pipe_task_done+0x5c/0xb0 [10136.669656] lima_gp_irq_handler+0xa8/0x120 [10136.669666] __handle_irq_event_percpu+0x48/0x160 [10136.669679] handle_irq_event+0x4c/0xc0 We can prevent that race condition entirely by masking the irqs at the beginning of the timeout handler, at which point we give up on waiting for that job entirely. The irqs will be enabled again at the next hard reset which is already done as a recovery by the timeout handler.	N/A	More Details
CVE-2024-6236	Denial of Service in NetScaler Console (formerly NetScaler ADM), NetScaler Agent, and NetScaler SDX	N/A	More Details
CVE-2024-40966	In the Linux kernel, the following vulnerability has been resolved: tty: add the option to have a tty reject a new ldisc ... and use it to limit the virtual terminals to just N_TTY. They are kind of special, and in particular, the "con_write()" routine violates the "writes cannot sleep" rule that some ldiscs rely on. This avoids the BUG: sleeping function called from invalid context at kernel/printk/printk.c:2659 when N_GSM has been attached to a virtual console, and gsmld_write() calls con_write() while holding a spinlock, and con_write() then tries to get the console lock.	N/A	More Details
CVE-2024-37405	Livechat messages can be leaked by combining two NoSQL injections affecting livechat:loginByToken (pre-authentication) and livechat:loadHistory.	N/A	More Details
CVE-2024-5912	An improper file signature check in Palo Alto Networks Cortex XDR agent may allow an attacker to bypass the Cortex XDR agent's executable blocking capabilities and run untrusted executables on the device. This issue can be leveraged to execute untrusted software without being detected or blocked.	N/A	More Details
CVE-2024-40978	In the Linux kernel, the following vulnerability has been resolved: scsi: qedi: Fix crash while reading debugfs attribute The qedi_dbg_do_not_recover_cmd_read() function invokes sprintf() directly on a __user pointer, which results into the crash. To fix this issue, use a small local stack buffer for sprintf() and then call simple_read_from_buffer(), which in turns make the copy_to_user() call. BUG: unable to handle page fault for address: 00007f4801111000 PGD 8000000864df6067 P4D 8000000864df6067 PUD 864df7067 PMD 846028067 PTE 0 Oops: 0002 [#1] PREEMPT SMP PTI Hardware name: HPE ProLiant DL380 Gen10/ProLiant DL380 Gen10, BIOS U30 06/15/2023 RIP: 0010:memcpy_orig+0xcd/0x130 RSP: 0018:ffffb7a18c3ffc40 EFLAGS: 00010202 RAX: 00007f4801111000 RBX: 00007f4801111000 RCX: 000000000000000f RDX: 000000000000000f RSI: ffffffffc0bfd7a0 RDI: 00007f4801111000 RBP: ffffffffc0bfd7a0 R08: 725f746f6e5f6f64 R09: 3d7265766f636572 R10: ffffb7a18c3ffd08 R11: 0000000000000000 R12: 00007f4881110fff R13: 000000007fffffff R14: ffffb7a18c3ffca0 R15: ffffffffc0bfd7af FS: 00007f480118a740(0000) GS:ffff98e38af00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f4801111000 CR3: 0000000864b8e001 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die_body+0x1a/0x60 ? page_fault_oops+0x183/0x510 ? exc_page_fault+0x69/0x150 ? asm_exc_page_fault+0x22/0x30 ? memcpy_orig+0xcd/0x130 vsnprintf+0x102/0x4c0 sprintf+0x51/0x80 qedi_dbg_do_not_recover_cmd_read+0x2f/0x50 [qedi 6bcfdeeecdea037da47069eca2ba717c84a77324] full_proxy_read+0x50/0x80 vfs_read+0xa5/0x2e0 ? folio_add_new_anon_rmap+0x44/0xa0 ? set_pte_at+0x15/0x30 ? do_pte_missing+0x426/0x7f0 ksys_read+0xa5/0xe0 do_syscall_64+0x58/0x80 ? __count_memcg_events+0x46/0x90 ? count_memcg_event_mm+0x3d/0x60 ? handle_mm_fault+0x196/0x2f0 ? do_user_addr_fault+0x267/0x890 ? exc_page_fault+0x69/0x150 entry_SYSCALL_64_after_hwframe+0x72/0xdc RIP: 0033:0x7f4800f20b4d	N/A	More Details
CVE-2024-6664	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2024-40963	In the Linux kernel, the following vulnerability has been resolved: mips: bmips: BCM6358: make sure CBR is correctly set It was discovered that some device have CBR address set to 0 causing kernel panic when arch_sync_dma_for_cpu_all is called. This was notice in situation where the system is booted from TP1 and BMIPS_GET_CBR() returns 0 instead of a valid address and !!(read_c0_brcm_cmt_local() & (1 << 31)); not failing. The current check whether RAC flush should be disabled or not are not enough hence lets check if CBR is a valid address or not.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40979	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix kernel crash during resume Currently during resume, QMI target memory is not properly handled, resulting in kernel crash in case DMA remap is not supported: BUG: Bad page state in process kworker/u16:54 pfn:36e80 page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x36e80 page dumped because: nonzero _refcount Call Trace: bad_page free_page_is_bad_report __free_pages_ok __free_pages dma_direct_free dma_free_attrs ath12k_qmi_free_target_mem_chunk ath12k_qmi_msg_mem_request_cb The reason is: Once ath12k module is loaded, firmware sends memory request to host. In case DMA remap not supported, ath12k refuses the first request due to failure in allocating with large segment size: ath12k_pci 0000:04:00.0: qmi firmware request memory request ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 7077888 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 8454144 ath12k_pci 0000:04:00.0: qmi dma allocation failed (7077888 B type 1), will try later with small size ath12k_pci 0000:04:00.0: qmi delays mem_request 2 ath12k_pci 0000:04:00.0: qmi firmware request memory request Later firmware comes back with more but small segments and allocation succeeds: ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 262144 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 524288 ath12k_pci 0000:04:00.0: qmi mem seg type 4 size 65536 ath12k_pci 0000:04:00.0: qmi mem seg type 1 size 524288 Now ath12k is working. If suspend is triggered, firmware will be reloaded during resume. As same as before, firmware requests two large segments at first. In ath12k_qmi_msg_mem_request_cb() segment count and size are assigned: ab->qmi.mem_seg_count == 2 ab->qmi.target_mem[0].size == 7077888 ab->qmi.target_mem[1].size == 8454144 Then allocation failed like before and ath12k_qmi_free_target_mem_chunk() is called to free all allocated segments. Note the first segment is skipped because its v.addr is cleared due to allocation failure: chunk->v.addr = dma_alloc_coherent() Also note that this leaks that segment because it has not been freed. While freeing the second segment, a size of 8454144 is passed to dma_free_coherent(). However remember that this segment is allocated at the first time firmware is loaded, before suspend. So its real size is 524288, much smaller than 8454144. As a result kernel found we are freeing some memory which is in use and thus cras ---truncated---	N/A	[More Details]()

CVE Number	Description	Base Score	Reference
CVE-2024-40962	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: allocate dummy checksums for zoned NODATASUM writes Shin'ichiro reported that when he's running fstests' test-case btrfs/167 on emulated zoned devices, he's seeing the following NULL pointer dereference in 'btrfs_zone_finish_endio()': Oops: general protection fault, probably for non-canonical address 0xdffffc0000000011: 0000 [#1] PREEMPT SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000088-0x000000000000008f] CPU: 4 PID: 2332440 Comm: kworker/u80:15 Tainted: G W 6.10.0-rc2-kts+ #4 Hardware name: Supermicro Super Server/X11SPi-TF, BIOS 3.3 02/21/2020 Workqueue: btrfs-endio-write btrfs_work_helper [btrfs] RIP: 0010:btrfs_zone_finish_endio.part.0+0x34/0x160 [btrfs] RSP: 0018:ffff88867f107a90 EFLAGS: 00010206 RAX: dffffc0000000000 RBX: 0000000000000000 RCX: ffffffff893e5534 RDX: 0000000000000011 RSI: 0000000000000004 RDI: 0000000000000088 RBP: 0000000000000002 R08: 0000000000000001 R09: ffffed1081696028 R10: ffff88840b4b0143 R11: ffff88834dfff600 R12: ffff88840b4b0000 R13: 0000000000020000 R14: 0000000000000000 R15: ffff888530ad5210 FS: 0000000000000000(0000) GS:ffff888e3f800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f87223fff38 CR3: 00000007a7c6a002 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0x27 ? die_addr+0x46/0x70 ? exc_general_protection+0x14f/0x250 ? asm_exc_general_protection+0x26/0x30 ? do_raw_read_unlock+0x44/0x70 ? btrfs_zone_finish_endio.part.0+0x34/0x160 [btrfs] btrfs_finish_one_ordered+0x5d9/0x19a0 [btrfs] ? __pfx_lock_release+0x10/0x10 ? do_raw_write_lock+0x90/0x260 ? __pfx_do_raw_write_lock+0x10/0x10 ? __pfx_btrfs_finish_one_ordered+0x10/0x10 [btrfs] ? _raw_write_unlock+0x23/0x40 ? btrfs_finish_ordered_zoned+0x5a9/0x850 [btrfs] ? lock_acquire+0x435/0x500 btrfs_work_helper+0x1b1/0xa70 [btrfs] ? __schedule+0x10a8/0x60b0 ? __pfx___might_resched+0x10/0x10 process_one_work+0x862/0x1410 ? __pfx_lock_acquire+0x10/0x10 ? __pfx_process_one_work+0x10/0x10 ? assign_work+0x16c/0x240 worker_thread+0x5e6/0x1010 ? __pfx_worker_thread+0x10/0x10 kthread+0x2c3/0x3a0 ? trace_irq_enable.constprop.0+0xce/0x110 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x31/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Enabling CONFIG_BTRFS_ASSERT revealed the following assertion to trigger: assertion failed: !list_empty(&ordered->list), in fs/btrfs/zoned.c:1815 This indicates, that we're missing the checksums list on the ordered_extent. As btrfs/167 is doing a NOCOW write this is to be expected. Further analysis with drgn confirmed the assumption: >>> inode = prog.crashed_thread().stack_trace()[11] ['ordered'].inode >>> btrfs_inode = drgn.container_of(inode, "struct btrfs_inode", \ "vfs_inode") >>> print(btrfs_inode.flags) (u32)1 As zoned emulation mode simulates conventional zones on regular devices, we cannot use zone-append for writing. But we're only attaching dummy checksums if we're doing a zone-append write. So for NOCOW zoned data writes on conventional zones, also attach a dummy checksum.	N/A	More Details
CVE-2024-40983	In the Linux kernel, the following vulnerability has been resolved: tipc: force a dst refcount before doing decryption As it says in commit 3bc07321ccc2 ("xfrm: Force a dst refcount before entering the xfrm type handlers"): "Crypto requests might return asynchronous. In this case we leave the rcu protected region, so force a refcount on the skb's destination entry before we enter the xfrm type input/output handlers." On TIPC decryption path it has the same problem, and skb_dst_force() should be called before doing decryption to avoid a possible crash. Shuang reported this issue when this warning is triggered: [] WARNING: include/net/dst.h:337 tipc_sk_rcv+0x1055/0x1ea0 [tipc] [] Kdump: loaded Tainted: G W --------- - - 4.18.0-496.el8.x86_64+debug [] Workqueue: crypto cryptd_queue_worker [] RIP: 0010:tipc_sk_rcv+0x1055/0x1ea0 [tipc] [] Call Trace: [] tipc_sk_mcast_rcv+0x548/0xea0 [tipc] [] tipc_rcv+0xcf5/0x1060 [tipc] [] tipc_aead_decrypt_done+0x215/0x2e0 [tipc] [] cryptd_aead_crypt+0xdb/0x190 [] cryptd_queue_worker+0xed/0x190 [] process_one_work+0x93d/0x17e0	N/A	More Details
CVE-2024-40984	In the Linux kernel, the following vulnerability has been resolved: ACPICA: Revert "ACPICA: avoid Info: mapping multiple BARs. Your kernel is fine." Undo the modifications made in commit d410ee5109a1 ("ACPICA: avoid "Info: mapping multiple BARs. Your kernel is fine.""). The initial purpose of this commit was to stop memory mappings for operation regions from overlapping page boundaries, as it can trigger warnings if different page attributes are present. However, it was found that when this situation arises, mapping continues until the boundary's end, but there is still an attempt to read/write the entire length of the map, leading to a NULL pointer deference. For example, if a four-byte mapping request is made but only one byte is mapped because it hits the current page boundary's end, a four-byte read/write attempt is still made, resulting in a NULL pointer deference. Instead, map the entire length, as the ACPI specification does not mandate that it must be within the same page boundary. It is permissible for it to be mapped across different regions.	N/A	More Details
CVE-2024-40985	In the Linux kernel, the following vulnerability has been resolved: net/tcp_ao: Don't leak ao_info on error-path It seems I introduced it together with TCP_AO_CMDF_AO_REQUIRED, on version 5 [1] of TCP-AO patches. Quite frustrative that having all these selftests that I've written, running kmemtest & kcov was always in todo. [1]: https://lore.kernel.org/netdev/20230215183335.800122-5-dima@arista.com/	N/A	More Details
CVE-2024-5911	An arbitrary file upload vulnerability in Palo Alto Networks Panorama software enables an authenticated read-write administrator with access to the web interface to disrupt system processes and crash the Panorama. Repeated attacks eventually cause the Panorama to enter maintenance mode, which requires manual intervention to bring the Panorama back online.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5492	Open redirect vulnerability allows a remote unauthenticated attacker to redirect users to arbitrary websites in NetScaler ADC and NetScaler Gateway	N/A	More Details
CVE-2024-5491	Denial of Service in NetScaler ADC and NetScaler Gateway in NetScaler	N/A	More Details
CVE-2024-40953	In the Linux kernel, the following vulnerability has been resolved: KVM: Fix a data race on last_boosted_vcpu in kvm_vcpu_on_spin() Use {READ,WRITE}_ONCE() to access kvm->last_boosted_vcpu to ensure the loads and stores are atomic. In the extremely unlikely scenario the compiler tears the stores, it's theoretically possible for KVM to attempt to get a vCPU using an out-of-bounds index, e.g. if the write is split into multiple 8-bit stores, and is paired with a 32-bit load on a VM with 257 vCPUs: CPU0 CPU1 last_boosted_vcpu = 0xff; (last_boosted_vcpu = 0x100) last_boosted_vcpu[15:8] = 0x01; i = (last_boosted_vcpu = 0x1ff) last_boosted_vcpu[7:0] = 0x00; vcpu = kvm->vcpu_array[0x1ff]; As detected by KCSAN: BUG: KCSAN: data-race in kvm_vcpu_on_spin [kvm] / kvm_vcpu_on_spin [kvm] write to 0xffffc90025a92344 of 4 bytes by task 4340 on cpu 16: kvm_vcpu_on_spin (arch/x86/kvm/../../../virt/kvm/kvm_main.c:4112) kvm handle_pause (arch/x86/kvm/vmx/vmx.c:5929) kvm_intel vmx_handle_exit (arch/x86/kvm/vmx/vmx.c:? arch/x86/kvm/vmx/vmx.c:6606) kvm_intel vcpu_run (arch/x86/kvm/x86.c:11107 arch/x86/kvm/x86.c:11211) kvm kvm_arch_vcpu_ioctl_run (arch/x86/kvm/x86.c:?) kvm kvm_vcpu_ioctl (arch/x86/kvm/../../../virt/kvm/kvm_main.c:?) kvm __se_sys_ioctl (fs/ioctl.c:52 fs/ioctl.c:904 fs/ioctl.c:890) __x64_sys_ioctl (fs/ioctl.c:890) x64_sys_call (arch/x86/entry/syscall_64.c:33) do_syscall_64 (arch/x86/entry/common.c:?) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) read to 0xffffc90025a92344 of 4 bytes by task 4342 on cpu 4: kvm_vcpu_on_spin (arch/x86/kvm/../../../virt/kvm/kvm_main.c:4069) kvm handle_pause (arch/x86/kvm/vmx/vmx.c:5929) kvm_intel vmx_handle_exit (arch/x86/kvm/vmx/vmx.c:? arch/x86/kvm/vmx/vmx.c:6606) kvm_intel vcpu_run (arch/x86/kvm/x86.c:11107 arch/x86/kvm/x86.c:11211) kvm kvm_arch_vcpu_ioctl_run (arch/x86/kvm/x86.c:?) kvm kvm_vcpu_ioctl (arch/x86/kvm/../../../virt/kvm/kvm_main.c:?) kvm __se_sys_ioctl (fs/ioctl.c:52 fs/ioctl.c:904 fs/ioctl.c:890) __x64_sys_ioctl (fs/ioctl.c:890) x64_sys_call (arch/x86/entry/syscall_64.c:33) do_syscall_64 (arch/x86/entry/common.c:?) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) value changed: 0x00000012 -> 0x00000000	N/A	More Details
CVE-2024-40986	In the Linux kernel, the following vulnerability has been resolved: dmaengine: xilinx: xdma: Fix data synchronisation in xdma_channel_isr() Requests the vchan lock before using xdma->stop_request.	N/A	More Details
CVE-2024-6663	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2024-6149	Redirection of users to a vulnerable URL in Citrix Workspace app for HTML5	N/A	More Details
CVE-2024-40987	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix UBSAN warning in kv_dpm.c Adds bounds check for sumo_vid_mapping_entry.	N/A	More Details
CVE-2024-6151	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Virtual Delivery Agent for Windows used by Citrix Virtual Apps and Desktops and Citrix DaaS	N/A	More Details
CVE-2024-6643	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-40940	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix tainted pointer delete is case of flow rules creation fail In case of flow rule creation fail in mlx5_lag_create_port_sel_table(), instead of previously created rules, the tainted pointer is deleted deveral times. Fix this bug by using correct flow rules pointers. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2024-36458	The vulnerability allows a malicious low-privileged PAM user to perform server upgrade related actions.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38495	A specific authentication strategy allows a malicious attacker to learn ids of all PAM users defined in its database.	N/A	More Details
CVE-2024-38494	This vulnerability allows a high-privileged authenticated PAM user to achieve remote command execution on the affected PAM system by sending a specially crafted HTTP request.	N/A	More Details
CVE-2024-38492	This vulnerability allows an unauthenticated attacker to achieve remote command execution on the affected PAM system by uploading a specially crafted PAM upgrade file.	N/A	More Details
CVE-2024-38491	The vulnerability allows an unauthenticated attacker to read arbitrary information from the database.	N/A	More Details
CVE-2022-48794	In the Linux kernel, the following vulnerability has been resolved: net: ieee802154: at86rf230: Stop leaking skb's Upon error the ieee802154_xmit_complete() helper is not called. Only ieee802154_wake_queue() is called manually. In the Tx case we then leak the skb structure. Free the skb structure upon error before returning when appropriate. As the 'is_tx = 0' cannot be moved in the complete handler because of a possible race between the delay in switching to STATE_RX_AACK_ON and a new interrupt, we introduce an intermediate 'was_tx' boolean just for this purpose. There is no Fixes tag applying here, many changes have been made on this area and the issue kind of always existed.	N/A	More Details
CVE-2022-48795	In the Linux kernel, the following vulnerability has been resolved: parisc: Fix data TLB miss in sba_unmap_sg Rolf Eike Beer reported the following bug: [1274934.746891] Bad Address (null pointer deref?): Code=15 (Data TLB miss fault) at addr 0000004140000018 [1274934.746891] CPU: 3 PID: 5549 Comm: cmake Not tainted 5.15.4-gentoo-parisc64 #4 [1274934.746891] Hardware name: 9000/785/C8000 [1274934.746891] [1274934.746891] YZrvWESTHLNXBCVMcbcbcbcbOGFRQPDI [1274934.746891] PSW: 00001000000001001111111000001110 Not tainted [1274934.746891] r00-03 000000ff0804fe0e 0000000040bc9bc0 00000000406760e4 0000004140000000 [1274934.746891] r04-07 0000000040b693c0 0000004140000000 000000004a2b08b0 0000000000000001 [1274934.746891] r08-11 0000000041f98810 0000000000000000 000000004a0a7000 0000000000000001 [1274934.746891] r12-15 0000000040bddbc0 0000000040c0cbc0 0000000040bddbc0 0000000040bddbc0 [1274934.746891] r16-19 0000000040bde3c0 0000000040bddbc0 0000000040bde3c0 0000000000000007 [1274934.746891] r20-23 0000000000000006 000000004a368950 0000000000000000 0000000000000001 [1274934.746891] r24-27 0000000000001fff 000000000800000e 000000004a1710f0 0000000040b693c0 [1274934.746891] r28-31 0000000000000001 0000000041f988b0 0000000041f98840 000000004a171118 [1274934.746891] sr00-03 00000000066e5800 0000000000000000 0000000000000000 00000000066e5800 [1274934.746891] sr04-07 0000000000000000 0000000000000000 0000000000000000 0000000000000000 [1274934.746891] [1274934.746891] IASQ: 0000000000000000 0000000000000000 IAOQ: 00000000406760e8 00000000406760ec [1274934.746891] IIR: 48780030 ISR: 0000000000000000 IOR: 0000004140000018 [1274934.746891] CPU: 3 CR30: 00000040e3a9c000 CR31: ffffffffffffffff [1274934.746891] ORIG_R28: 0000000040acdd58 [1274934.746891] IAOQ[0]: sba_unmap_sg+0xb0/0x118 [1274934.746891] IAOQ[1]: sba_unmap_sg+0xb4/0x118 [1274934.746891] RP(r2): sba_unmap_sg+0xac/0x118 [1274934.746891] Backtrace: [1274934.746891] [<00000000402740cc>] dma_unmap_sg_attrs+0x6c/0x70 [1274934.746891] [<000000004074d6bc>] scsi_dma_unmap+0x54/0x60 [1274934.746891] [<00000000407a3488>] mptscsih_io_done+0x150/0xd70 [1274934.746891] [<0000000040798600>] mpt_interrupt+0x168/0xa68 [1274934.746891] [<0000000040255a48>] __handle_irq_event_percpu+0xc8/0x278 [1274934.746891] [<0000000040255c34>] handle_irq_event_percpu+0x3c/0xd8 [1274934.746891] [<000000004025ecb4>] handle_percpu_irq+0xb4/0xf0 [1274934.746891] [<00000000402548e0>] generic_handle_irq+0x50/0x70 [1274934.746891] [<000000004019a254>] call_on_stack+0x18/0x24 [1274934.746891] [1274934.746891] Kernel panic - not syncing: Bad Address (null pointer deref?) The bug is caused by overrunning the sglist and incorrectly testing sg_dma_len(sglist) before nents. Normally this doesn't cause a crash, but in this case sglist crossed a page boundary. This occurs in the following code: while (sg_dma_len(sglist) && nents--) { The fix is simply to test nents first and move the decrement of nents into the loop.	N/A	More Details
CVE-2024-6677	Privilege escalation in uberAgent	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48797	In the Linux kernel, the following vulnerability has been resolved: mm: don't try to NUMA-migrate COW pages that have other uses Oded Gabbay reports that enabling NUMA balancing causes corruption with his Gaudi accelerator test load: "All the details are in the bug, but the bottom line is that somehow, this patch causes corruption when the numa balancing feature is enabled AND we don't use process affinity AND we use GUP to pin pages so our accelerator can DMA to/from system memory. Either disabling numa balancing, using process affinity to bind to specific numa-node or reverting this patch causes the bug to disappear" and Oded bisected the issue to commit 09854ba94c6a ("mm: do_wp_page() simplification"). Now, the NUMA balancing shouldn't actually be changing the writability of a page, and as such shouldn't matter for COW. But it appears it does. Suspicious. However, regardless of that, the condition for enabling NUMA faults in change_pte_range() is nonsensical. It uses "page_mapcount(page)" to decide if a COW page should be NUMA-protected or not, and that makes absolutely no sense. The number of mappings a page has is irrelevant: not only does GUP get a reference to a page as in Oded's case, but the other mappings migth be paged out and the only reference to them would be in the page count. Since we should never try to NUMA-balance a page that we can't move anyway due to other references, just fix the code to use 'page_count()'. Oded confirms that that fixes his issue. Now, this does imply that something in NUMA balancing ends up changing page protections (other than the obvious one of making the page inaccessible to get the NUMA faulting information). Otherwise the COW simplification wouldn't matter - since doing the GUP on the page would make sure it's writable. The cause of that permission change would be good to figure out too, since it clearly results in spurious COW events - but fixing the nonsensical test that just happened to work before is obviously the CorrectThing(tm) to do regardless.	N/A	More Details
CVE-2022-48798	In the Linux kernel, the following vulnerability has been resolved: s390/cio: verify the driver availability for path_event call If no driver is attached to a device or the driver does not provide the path_event function, an FCES path-event on this device could end up in a kernel-panic. Verify the driver availability before the path_event function call.	N/A	More Details
CVE-2022-48799	In the Linux kernel, the following vulnerability has been resolved: perf: Fix list corruption in perf_cgroup_switch() There's list corruption on cgrp_cpuctx_list. This happens on the following path: perf_cgroup_switch: list_for_each_entry(cgrp_cpuctx_list) cpu_ctx_sched_in ctx_sched_in ctx_pinned_sched_in merge_sched_in perf_cgroup_event_disable: remove the event from the list Use list_for_each_entry_safe() to allow removing an entry during iteration.	N/A	More Details
CVE-2022-48801	In the Linux kernel, the following vulnerability has been resolved: iio: buffer: Fix file related error handling in IIO_BUFFER_GET_FD_IOCTL If we fail to copy the just created file descriptor to userland, we try to clean up by putting back 'fd' and freeing 'ib'. The code uses put_unused_fd() for the former which is wrong, as the file descriptor was already published by fd_install() which gets called internally by anon_inode_getfd(). This makes the error handling code leaving a half cleaned up file descriptor table around and a partially destructed 'file' object, allowing userland to play use-after-free tricks on us, by abusing the still usable fd and making the code operate on a dangling 'file->private_data' pointer. Instead of leaving the kernel in a partially corrupted state, don't attempt to explicitly clean up and leave this to the process exit path that'll release any still valid fds, including the one created by the previous call to anon_inode_getfd(). Simply return -EFAULT to indicate the error.	N/A	More Details
CVE-2024-6642	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48802	In the Linux kernel, the following vulnerability has been resolved: fs/proc: task_mmu.c: don't read mapcount for migration entry The syzbot reported the below BUG: kernel BUG at include/linux/page-flags.h:785! invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 PID: 4392 Comm: syz-executor560 Not tainted 5.16.0-rc6-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:PageDoubleMap include/linux/page-flags.h:785 [inline] RIP: 0010:__page_mapcount+0x2d2/0x350 mm/util.c:744 Call Trace: page_mapcount include/linux/mm.h:837 [inline] smaps_account+0x470/0xb10 fs/proc/task_mmu.c:466 smaps_pte_entry fs/proc/task_mmu.c:538 [inline] smaps_pte_range+0x611/0x1250 fs/proc/task_mmu.c:601 walk_pmd_range mm/pagewalk.c:128 [inline] walk_pud_range mm/pagewalk.c:205 [inline] walk_p4d_range mm/pagewalk.c:240 [inline] walk_pgd_range mm/pagewalk.c:277 [inline] __walk_page_range+0xe23/0x1ea0 mm/pagewalk.c:379 walk_page_vma+0x277/0x350 mm/pagewalk.c:530 smap_gather_stats.part.0+0x148/0x260 fs/proc/task_mmu.c:768 smap_gather_stats fs/proc/task_mmu.c:741 [inline] show_smap+0xc6/0x440 fs/proc/task_mmu.c:822 seq_read_iter+0xbb0/0x1240 fs/seq_file.c:272 seq_read+0x3e0/0x5b0 fs/seq_file.c:162 vfs_read+0x1b5/0x600 fs/read_write.c:479 ksys_read+0x12d/0x250 fs/read_write.c:619 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae The reproducer was trying to read /proc/$PID/smaps when calling MADV_FREE at the mean time. MADV_FREE may split THPs if it is called for partial THP. It may trigger the below race: CPU A CPU B ----- ----- smaps walk: MADV_FREE: page_mapcount() PageCompound() split_huge_page() page = compound_head(page) PageDoubleMap(page) When calling PageDoubleMap() this page is not a tail page of THP anymore so the BUG is triggered. This could be fixed by elevated refcount of the page before calling mapcount, but that would prevent it from counting migration entries, and it seems overkilling because the race just could happen when PMD is split so all PTE entries of tail pages are actually migration entries, and smaps_account() does treat migration entries as mapcount == 1 as Kirill pointed out. Add a new parameter for smaps_account() to tell this entry is migration entry then skip calling page_mapcount(). Don't skip getting mapcount for device private entries since they do track references with mapcount. Pagemap also has the similar issue although it was not reported. Fixed it as well. [shy828301@gmail.com: v4] Link: https://lkml.kernel.org/r/20220203182641.824731-1-shy828301@gmail.com [nathan@kernel.org: avoid unused variable warning in pagemap_pmd_range()] Link: https://lkml.kernel.org/r/20220207171049.1102239-1-nathan@kernel.org	N/A	More Details
CVE-2022-48803	In the Linux kernel, the following vulnerability has been resolved: phy: ti: Fix missing sentinel for clk_div_table _get_table_maxdiv() tries to access "clk_div_table" array out of bound defined in phy-j721e-wiz.c. Add a sentinel entry to prevent the following global-out-of-bounds error reported by enabling KASAN. [9.552392] BUG: KASAN: global-out-of-bounds in _get_maxdiv+0xc0/0x148 [9.558948] Read of size 4 at addr ffff8000095b25a4 by task kworker/u4:1/38 [9.565926] [9.567441] CPU: 1 PID: 38 Comm: kworker/u4:1 Not tainted 5.16.0-116492-gdaadb3bd0e8d-dirty #360 [9.576242] Hardware name: Texas Instruments J721e EVM (DT) [9.581832] Workqueue: events_unbound deferred_probe_work_func [9.587708] Call trace: [9.590174] dump_backtrace+0x20c/0x218 [9.594038] show_stack+0x18/0x68 [9.597375] dump_stack_lvl+0x9c/0xd8 [9.601062] print_address_description.constprop.0+0x78/0x334 [9.606830] kasan_report+0x1f0/0x260 [9.610517] __asan_load4+0x9c/0xd8 [9.614030] _get_maxdiv+0xc0/0x148 [9.617540] divider_determine_rate+0x88/0x488 [9.622005] divider_round_rate_parent+0xc8/0x124 [9.626729] wiz_clk_div_round_rate+0x54/0x68 [9.631113] clk_core_determine_round_nolock+0x124/0x158 [9.636448] clk_core_round_rate_nolock+0x68/0x138 [9.641260] clk_core_set_rate_nolock+0x268/0x3a8 [9.645987] clk_set_rate+0x50/0xa8 [9.649499] cdns_sierra_phy_init+0x88/0x248 [9.653794] phy_init+0x98/0x108 [9.657046] cdns_pcie_enable_phy+0xa0/0x170 [9.661340] cdns_pcie_init_phy+0x250/0x2b0 [9.665546] j721e_pcie_probe+0x4b8/0x798 [9.669579] platform_probe+0x8c/0x108 [9.673350] really_probe+0x114/0x630 [9.677037] __driver_probe_device+0x18c/0x220 [9.681505] driver_probe_device+0xac/0x150 [9.685712] __device_attach_driver+0xec/0x170 [9.690178] bus_for_each_drv+0xf0/0x158 [9.694124] __device_attach+0x184/0x210 [9.698070] device_initial_probe+0x14/0x20 [9.702277] bus_probe_device+0xec/0x100 [9.706223] deferred_probe_work_func+0x124/0x180 [9.710951] process_one_work+0x4b0/0xbc0 [9.714983] worker_thread+0x74/0x5d0 [9.718668] kthread+0x214/0x230 [9.721919] ret_from_fork+0x10/0x20 [9.725520] [9.727032] The buggy address belongs to the variable: [9.732183] clk_div_table+0x24/0x440	N/A	More Details
CVE-2024-36457	The vulnerability allows an attacker to bypass the authentication requirements for a specific PAM endpoint.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48805	In the Linux kernel, the following vulnerability has been resolved: net: usb: ax88179_178a: Fix out-of-bounds accesses in RX fixup ax88179_rx_fixup() contains several out-of-bounds accesses that can be triggered by a malicious (or defective) USB device, in particular: - The metadata array (hdr_off..hdr_off+2*pkt_cnt) can be out of bounds, causing OOB reads and (on big-endian systems) OOB endianness flips. - A packet can overlap the metadata array, causing a later OOB endianness flip to corrupt data used by a cloned SKB that has already been handed off into the network stack. - A packet SKB can be constructed whose tail is far beyond its end, causing out-of-bounds heap data to be considered part of the SKB's data. I have tested that this can be used by a malicious USB device to send a bogus ICMPv6 Echo Request and receive an ICMPv6 Echo Reply in response that contains random kernel heap data. It's probably also possible to get OOB writes from this on a little-endian system somehow - maybe by triggering skb_cow() via IP options processing -, but I haven't tested that.	N/A	More Details
CVE-2022-48806	In the Linux kernel, the following vulnerability has been resolved: eeprom: ee1004: limit i2c reads to I2C_SMBUS_BLOCK_MAX Commit effa453168a7 ("i2c: i801: Don't silently correct invalid transfer size") revealed that ee1004_eeprom_read() did not properly limit how many bytes to read at once. In particular, i2c_smbus_read_i2c_block_data_or_emulated() takes the length to read as an u8. If count == 256 after taking into account the offset and page boundary, the cast to u8 overflows. And this is common when user space tries to read the entire EEPROM at once. To fix it, limit each read to I2C_SMBUS_BLOCK_MAX (32) bytes, already the maximum length i2c_smbus_read_i2c_block_data_or_emulated() allows.	N/A	More Details
CVE-2022-48807	In the Linux kernel, the following vulnerability has been resolved: ice: Fix KASAN error in LAG NETDEV_UNREGISTER handler Currently, the same handler is called for both a NETDEV_BONDING_INFO LAG unlink notification as for a NETDEV_UNREGISTER call. This is causing a problem though, since the netdev_notifier_info passed has a different structure depending on which event is passed. The problem manifests as a call trace from a BUG: KASAN stack-out-of-bounds error. Fix this by creating a handler specific to NETDEV_UNREGISTER that only is passed valid elements in the netdev_notifier_info struct for the NETDEV_UNREGISTER event. Also included is the removal of an unbalanced dev_put on the peer_netdev and related braces.	N/A	More Details
CVE-2024-36456	This vulnerability allows an unauthenticated attacker to achieve remote command execution on the affected PAM system by uploading a specially crafted PAM upgrade file.	N/A	More Details
CVE-2024-36455	An improper input validation allows an unauthenticated attacker to achieve remote command execution on the affected PAM system by sending a specially crafted HTTP request.	N/A	More Details
CVE-2022-48810	In the Linux kernel, the following vulnerability has been resolved: ipmr,ip6mr: acquire RTNL before calling ip[6]mr_free_table() on failure path ip[6]mr_free_table() can only be called under RTNL lock. RTNL: assertion failed at net/core/dev.c (10367) WARNING: CPU: 1 PID: 5890 at net/core/dev.c:10367 unregister_netdevice_many+0x1246/0x1850 net/core/dev.c:10367 Modules linked in: CPU: 1 PID: 5890 Comm: syz-executor.2 Not tainted 5.16.0-syzkaller-11627-g422ee58dc0ef #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:unregister_netdevice_many+0x1246/0x1850 net/core/dev.c:10367 Code: 0f 85 9b ee ff ff e8 69 07 4b fa ba 7f 28 00 00 48 c7 c6 00 90 ae 8a 48 c7 c7 40 90 ae 8a c6 05 6d b1 51 06 01 e8 8c 90 d8 01 <0f> 0b e9 70 ee ff ff e8 3e 07 4b fa 4c 89 e7 e8 86 2a 59 fa e9 ee RSP: 0018:ffffc900046ff6e0 EFLAGS: 00010286 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000 RDX: ffff888050f51d00 RSI: ffffffff815fa008 RDI: fffff520008dfece RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000 R10: ffffffff815f3d6e R11: 0000000000000000 R12: 00000000ffffffff4 R13: dffffc0000000000 R14: ffffc900046ff750 R15: ffff88807b7dc000 FS: 00007f4ab736e700(0000) GS:ffff8880b9d00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fee0b4f8990 CR3: 000000001e7d2000 CR4: 00000000003506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> mroute_clean_tables+0x244/0xb40 net/ipv6/ip6mr.c:1509 ip6mr_free_table net/ipv6/ip6mr.c:389 [inline] ip6mr_rules_init net/ipv6/ip6mr.c:246 [inline] ip6mr_net_init net/ipv6/ip6mr.c:1306 [inline] ip6mr_net_init+0x3f0/0x4e0 net/ipv6/ip6mr.c:1298 ops_init+0xaf/0x470 net/core/net_namespace.c:140 setup_net+0x54f/0xbb0 net/core/net_namespace.c:331 copy_net_ns+0x318/0x760 net/core/net_namespace.c:475 create_new_namespaces+0x3f6/0xb20 kernel/nsproxy.c:110 copy_namespaces+0x391/0x450 kernel/nsproxy.c:178 copy_process+0x2e0c/0x7300 kernel/fork.c:2167 kernel_clone+0xe7/0xab0 kernel/fork.c:2555 __do_sys_clone+0xc8/0x110 kernel/fork.c:2672 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f4ab89f9059 Code: Unable to access opcode bytes at RIP 0x7f4ab89f902f. RSP: 002b:00007f4ab736e118 EFLAGS: 00000206 ORIG_RAX: 0000000000000038 RAX: ffffffffffffffda RBX: 00007f4ab8b0bf60 RCX: 00007f4ab89f9059 RDX: 0000000020000280 RSI: 0000000020000270 RDI: 0000000040200000 RBP: 00007f4ab8a5308d R08: 0000000020000300 R09: 0000000020000300 R10: 00000000200002c0 R11: 0000000000000206 R12: 0000000000000000 R13: 00007ffc3977cc1f R14: 00007f4ab736e300 R15: 0000000000022000 </TASK>	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48811	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: don't release napi in __ibmvnic_open() If __ibmvnic_open() encounters an error such as when setting link state, it calls release_resources() which frees the napi structures needlessly. Instead, have __ibmvnic_open() only clean up the work it did so far (i.e. disable napi and irqs) and leave the rest to the callers. If caller of __ibmvnic_open() is ibmvnic_open(), it should release the resources immediately. If the caller is do_reset() or do_hard_reset(), they will release the resources on the next reset. This fixes following crash that occurred when running the drmgr command several times to add/remove a vnic interface: [102056] ibmvnic 30000003 env3: Disabling rx_scrq[6] irq [102056] ibmvnic 30000003 env3: Disabling rx_scrq[7] irq [102056] ibmvnic 30000003 env3: Replenished 8 pools Kernel attempted to read user page (10) - exploit attempt? (uid: 0) BUG: Kernel NULL pointer dereference on read at 0x00000010 Faulting instruction address: 0xc000000000a3c840 Oops: Kernel access of bad area, sig: 11 [#1] LE PAGE_SIZE=64K MMU=Radix SMP NR_CPUS=2048 NUMA pSeries ... CPU: 9 PID: 102056 Comm: kworker/9:2 Kdump: loaded Not tainted 5.16.0-rc5-autotest-g6441998e2e37 #1 Workqueue: events_long __ibmvnic_reset [ibmvnic] NIP: c000000000a3c840 LR: c0080000029b5378 CTR: c000000000a3c820 REGS: c0000000548e37e0 TRAP: 0300 Not tainted (5.16.0-rc5-autotest-g6441998e2e37) MSR: 8000000000009033 <SF,EE,ME,IR,DR,RI,LE> CR: 28248484 XER: 00000004 CFAR: c0080000029bdd24 DAR: 0000000000000010 DSISR: 40000000 IRQMASK: 0 GPR00: c0080000029b55d0 c0000000548e3a80 c0000000028f0200 0000000000000000 ... NIP [c000000000a3c840] napi_enable+0x20/0xc0 LR [c0080000029b5378] __ibmvnic_open+0xf0/0x430 [ibmvnic] Call Trace: [c0000000548e3a80] [0000000000000006] 0x6 (unreliable) [c0000000548e3ab0] [c0080000029b55d0] __ibmvnic_open+0x348/0x430 [ibmvnic] [c0000000548e3b40] [c0080000029bcc28] __ibmvnic_reset+0x500/0xdf0 [ibmvnic] [c0000000548e3c60] [c000000000176228] process_one_work+0x288/0x570 [c0000000548e3d00] [c000000000176588] worker_thread+0x78/0x660 [c0000000548e3da0] [c0000000001822f0] kthread+0x1c0/0x1d0 [c0000000548e3e10] [c00000000000cf64] ret_from_kernel_thread+0x5c/0x64 Instruction dump: 7d2948f8 792307e0 4e800020 60000000 3c4c01eb 384239e0 f821ffd1 39430010 38a0fff6 e92d1100 f9210028 39200000 <e9030010> f9010020 60420000 e9210020 ---[end trace 5f8033b08fd27706]---	N/A	More Details
CVE-2024-38496	The vulnerability allows a malicious low-privileged PAM user to access information about other PAM users and their group memberships.	N/A	More Details
CVE-2024-6716	Rejected reason: Invalid security issue.	N/A	More Details
CVE-2024-40908	In the Linux kernel, the following vulnerability has been resolved: bpf: Set run context for rawtp test_run callback syzbot reported crash when rawtp program executed through the test_run interface calls bpf_get_attach_cookie helper or any other helper that touches task->bpf_ctx pointer. Setting the run context (task->bpf_ctx pointer) for test_run callback.	N/A	More Details
CVE-2022-48786	In the Linux kernel, the following vulnerability has been resolved: vsock: remove vsock from connected table when connect is interrupted by a signal vsock_connect() expects that the socket could already be in the TCP_ESTABLISHED state when the connecting task wakes up with a signal pending. If this happens the socket will be in the connected table, and it is not removed when the socket state is reset. In this situation it's common for the process to retry connect(), and if the connection is successful the socket will be added to the connected table a second time, corrupting the list. Prevent this by calling vsock_remove_connected() if a signal is received while waiting for a connection. This is harmless if the socket is not in the connected table, and if it is in the table then removing it will prevent list corruption from a double add. Note for backporting: this patch requires d5afa82c977e ("vsock: correct removal of socket from the list"), which is in all current stable trees except 4.9.y.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39502	In the Linux kernel, the following vulnerability has been resolved: ionic: fix use after netif_napi_del() When queues are started, netif_napi_add() and napi_enable() are called. If there are 4 queues and only 3 queues are used for the current configuration, only 3 queues' napi should be registered and enabled. The ionic_qcq_enable() checks whether the .poll pointer is not NULL for enabling only the using queue' napi. Unused queues' napi will not be registered by netif_napi_add(), so the .poll pointer indicates NULL. But it couldn't distinguish whether the napi was unregistered or not because netif_napi_del() doesn't reset the .poll pointer to NULL. So, ionic_qcq_enable() calls napi_enable() for the queue, which was unregistered by netif_napi_del(). Reproducer: ethtool -L <interface name> rx 1 tx 1 combined 0 ethtool -L <interface name> rx 0 tx 0 combined 1 ethtool -L <interface name> rx 0 tx 0 combined 4 Splat looks like: kernel BUG at net/core/dev.c:6666! Oops: invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 1057 Comm: kworker/3:3 Not tainted 6.10.0-rc2+ #16 Workqueue: events ionic_lif_deferred_work [ionic] RIP: 0010:napi_enable+0x3b/0x40 Code: 48 89 c2 48 83 e2 f6 80 b9 61 09 00 00 00 74 0d 48 83 bf 60 01 00 00 00 74 03 80 ce 01 f0 4f RSP: 0018:ffffb6ed83227d48 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff97560cda0828 RCX: 0000000000000029 RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffff97560cda0a28 RBP: ffffb6ed83227d50 R08: 0000000000000400 R09: 0000000000000001 R10: 0000000000000001 R11: 0000000000000001 R12: 0000000000000000 R13: ffff97560ce3c1a0 R14: 0000000000000000 R15: ffff975613ba0a20 FS: 0000000000000000(0000) GS:ffff975d5f780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f8f734ee200 CR3: 0000000103e50000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <TASK> ? die+0x33/0x90 ? do_trap+0xd9/0x100 ? napi_enable+0x3b/0x40 ? do_error_trap+0x83/0xb0 ? napi_enable+0x3b/0x40 ? napi_enable+0x3b/0x40 ? exc_invalid_op+0x4e/0x70 ? napi_enable+0x3b/0x40 ? asm_exc_invalid_op+0x16/0x20 ? napi_enable+0x3b/0x40 ionic_qcq_enable+0xb7/0x180 [ionic 59bdfc8a035436e1c4224ff7d10789e3f14643f8] ionic_start_queues+0xc4/0x290 [ionic 59bdfc8a035436e1c4224ff7d10789e3f14643f8] ionic_link_status_check+0x11c/0x170 [ionic 59bdfc8a035436e1c4224ff7d10789e3f14643f8] ionic_lif_deferred_work+0x129/0x280 [ionic 59bdfc8a035436e1c4224ff7d10789e3f14643f8] process_one_work+0x145/0x360 worker_thread+0x2bb/0x3d0 ? __pfx_worker_thread+0x10/0x10 kthread+0xcc/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2024-39501	In the Linux kernel, the following vulnerability has been resolved: drivers: core: synchronize really_probe() and dev_uevent() Synchronize the dev->driver usage in really_probe() and dev_uevent(). These can run in different threads, what can result in the following race condition for dev->driver uninitialization: Thread #1: ========== really_probe() { ... probe_failed: ... device_unbind_cleanup(dev) { ... dev->driver = NULL; // <= Failed probe sets dev->driver to NULL ... } ... } Thread #2: ========== dev_uevent() { ... if (dev->driver) // If dev->driver is NULLed from really_probe() from here on, // after above check, the system crashes add_uevent_var(env, "DRIVER=%s", dev->driver->name); ... } really_probe() holds the lock, already. So nothing needs to be done there. dev_uevent() is called with lock held, often, too. But not always. What implies that we can't add any locking in dev_uevent() itself. So fix this race by adding the lock to the non-protected path. This is the path where above race is observed: dev_uevent+0x235/0x380 uevent_show+0x10c/0x1f0 <= Add lock here dev_attr_show+0x3a/0xa0 sysfs_kf_seq_show+0x17c/0x250 kernfs_seq_show+0x7c/0x90 seq_read_iter+0x2d7/0x940 kernfs_fop_read_iter+0xc6/0x310 vfs_read+0x5bc/0x6b0 ksys_read+0xeb/0x1b0 __x64_sys_read+0x42/0x50 x64_sys_call+0x27ad/0x2d30 do_syscall_64+0xcd/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Similar cases are reported by syzkaller in https://syzkaller.appspot.com/bug?extid=ffa8143439596313a85a But these are regarding the *initialization* of dev->driver dev->driver = drv; As this switches dev->driver to non-NULL these reports can be considered to be false-positives (which should be "fixed" by this commit, as well, though). The same issue was reported and tried to be fixed back in 2015 in https://lore.kernel.org/lkml/1421259054-2574-1-git-send-email-a.sangwan@samsung.com/ already.	N/A	More Details
CVE-2024-41008	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: change vm->task_info handling This patch changes the handling and lifecycle of vm->task_info object. The major changes are: - vm->task_info is a dynamically allocated ptr now, and its uasge is reference counted. - introducing two new helper funcs for task_info lifecycle management - amdgpu_vm_get_task_info: reference counts up task_info before returning this info - amdgpu_vm_put_task_info: reference counts down task_info - last put to task_info() frees task_info from the vm. This patch also does logistical changes required for existing usage of vm->task_info. V2: Do not block all the prints when task_info not found (Felix) V3: Fixed review comments from Felix - Fix wrong indentation - No debug message for -ENOMEM - Add NULL check for task_info - Do not duplicate the debug messages (ti vs no ti) - Get first reference of task_info in vm_init(), put last in vm_fini() V4: Fixed review comments from Felix - fix double reference increment in create_task_info - change amdgpu_vm_get_task_info_pasid - additional changes in amdgpu_gem.c while porting	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39500	In the Linux kernel, the following vulnerability has been resolved: sock_map: avoid race between sock_map_close and sk_psock_put sk_psock_get will return NULL if the refcount of psock has gone to 0, which will happen when the last call of sk_psock_put is done. However, sk_psock_drop may not have finished yet, so the close callback will still point to sock_map_close despite psock being NULL. This can be reproduced with a thread deleting an element from the sock map, while the second one creates a socket, adds it to the map and closes it. That will trigger the WARN_ON_ONCE: ----------[cut here]------------ WARNING: CPU: 1 PID: 7220 at net/core/sock_map.c:1701 sock_map_close+0x2a2/0x2d0 net/core/sock_map.c:1701 Modules linked in: CPU: 1 PID: 7220 Comm: syz-executor380 Not tainted 6.9.0-syzkaller-07726-g3c999d1ae3c7 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/02/2024 RIP: 0010:sock_map_close+0x2a2/0x2d0 net/core/sock_map.c:1701 Code: df e8 92 29 88 f8 48 8b 1b 48 89 d8 48 c1 e8 03 42 80 3c 20 00 74 08 48 89 df e8 79 29 88 f8 4c 8b 23 eb 89 e8 4f 15 23 f8 90 <0f> 0b 90 48 83 c4 08 5b 41 5c 41 5d 41 5e 41 5f 5d e9 13 26 3d 02 RSP: 0018:ffffc9000441fda8 EFLAGS: 00010293 RAX: ffffffff89731ae1 RBX: ffffffff94b87540 RCX: ffff888029470000 RDX: 0000000000000000 RSI: ffffffff8bcab5c0 RDI: ffffffff8c1faba0 RBP: 0000000000000000 R08: ffffffff92f9b61f R09: 1ffffffff25f36c3 R10: dffffc0000000000 R11: fffffbfff25f36c4 R12: ffffffff89731840 R13: ffff88804b587000 R14: ffff88804b587000 R15: ffffffff89731870 FS: 000055555e080380(0000) GS:ffff8880b9500000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000000207d4000 CR4: 0000000000350ef0 Call Trace: <TASK> unix_release+0x87/0xc0 net/unix/af_unix.c:1048 __sock_release net/socket.c:659 [inline] sock_close+0xbe/0x240 net/socket.c:1421 __fput+0x42b/0x8a0 fs/file_table.c:422 __do_sys_close fs/open.c:1556 [inline] __se_sys_close fs/open.c:1541 [inline] __x64_sys_close+0x7f/0x110 fs/open.c:1541 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf5/0x240 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fb37d618070 Code: 00 00 48 c7 c2 b8 ff ff ff f7 d8 64 89 02 b8 ff ff ff ff eb d4 e8 10 2c 00 00 80 3d 31 f0 07 00 00 74 17 b8 03 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 48 c3 0f 1f 80 00 00 00 00 48 83 ec 18 89 7c RSP: 002b:00007ffcd4a525d8 EFLAGS: 00000202 ORIG_RAX: 0000000000000003 RAX: ffffffffffffffda RBX: 0000000000000005 RCX: 00007fb37d618070 RDX: 0000000000000010 RSI: 00000000200001c0 RDI: 0000000000000004 RBP: 0000000000000000 R08: 0000000100000000 R09: 0000000100000000 R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 </TASK> Use sk_psock, which will only check that the pointer is not been set to NULL yet, which should only happen after the callbacks are restored. If, then, a reference can still be gotten, we may call sk_psock_stop and cancel psock->work. As suggested by Paolo Abeni, reorder the condition so the control flow is less convoluted. After that change, the reproducer does not trigger the WARN_ON_ONCE anymore.	N/A	More Details
CVE-2024-39499	In the Linux kernel, the following vulnerability has been resolved: vmci: prevent speculation leaks by sanitizing event in event_deliver() Coverity spotted that event_msg is controlled by user-space, event_msg->event_data.event is passed to event_deliver() and used as an index without sanitization. This change ensures that the event index is sanitized to mitigate any possibility of speculative information leaks. This bug was discovered and resolved using Coverity Static Analysis Security Testing (SAST) by Synopsys, Inc. Only compile tested, no access to HW.	N/A	More Details
CVE-2024-39497	In the Linux kernel, the following vulnerability has been resolved: drm/shmem-helper: Fix BUG_ON() on mmap(PROT_WRITE, MAP_PRIVATE) Lack of check for copy-on-write (COW) mapping in drm_gem_shmem_mmap allows users to call mmap with PROT_WRITE and MAP_PRIVATE flag causing a kernel panic due to BUG_ON in vmf_insert_pfn_prot: BUG_ON((vma->vm_flags & VM_PFNMAP) && is_cow_mapping(vma->vm_flags)); Return -EINVAL early if COW mapping is detected. This bug affects all drm drivers using default shmem helpers. It can be reproduced by this simple example: void *ptr = mmap(0, size, PROT_WRITE, MAP_PRIVATE, fd, mmap_offset); ptr[0] = 0;	N/A	More Details
CVE-2024-39503	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: Fix race between namespace cleanup and gc in the list:set type Lion Ackermann reported that there is a race condition between namespace cleanup in ipset and the garbage collection of the list:set type. The namespace cleanup can destroy the list:set type of sets while the gc of the set type is waiting to run in rcu cleanup. The latter uses data from the destroyed set which thus leads use after free. The patch contains the following parts: - When destroying all sets, first remove the garbage collectors, then wait if needed and then destroy the sets. - Fix the badly ordered "wait then remove gc" for the destroy a single set case. - Fix the missing rcu locking in the list:set type in the userspace test case. - Use proper RCU list handlings in the list:set type. The patch depends on c1193d9bbbd3 (netfilter: ipset: Add list flush to cancel_gc).	N/A	More Details
CVE-2024-3798	Insecure handling of GET header parameter file included in requests being sent to an instance of the open-source project Phoniebox allows an attacker to create a website, which – when visited by a user – will send malicious requests to multiple hosts on the local network. If such a request reaches the server, it will cause one of the following (depending on the chosen payload): shell command execution, reflected XSS or cross-site request forgery. This issue affects Phoniebox in all releases through 2.7. Newer 2.x releases were not tested, but they might also be vulnerable. Phoniebox in version 3.0 and higher are not affected.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40998	In the Linux kernel, the following vulnerability has been resolved: ext4: fix uninitialized ratelimit_state->lock access in __ext4_fill_super() In the following concurrency we will access the uninitialized rs->lock: ext4_fill_super ext4_register_sysfs // sysfs registered msg_ratelimit_interval_ms // Other processes modify rs->interval to // non-zero via msg_ratelimit_interval_ms ext4_orphan_cleanup ext4_msg(sb, KERN_INFO, "Errors on filesystem, " __ext4_msg ___ratelimit(&(EXT4_SB(sb)->s_msg_ratelimit_state) if (!rs->interval) // do nothing if interval is 0 return 1; raw_spin_trylock_irqsave(&rs->lock, flags) raw_spin_trylock(lock) _raw_spin_trylock __raw_spin_trylock spin_acquire(&lock->dep_map, 0, 1, _RET_IP_) lock_acquire __lock_acquire register_lock_class assign_lock_key dump_stack(); ratelimit_state_init(&sbi->s_msg_ratelimit_state, 5 * HZ, 10); raw_spin_lock_init(&rs->lock); // init rs->lock here and get the following dump_stack: == INFO: trying to register non-static key. The code is fine but needs lockdep annotation, or maybe you didn't initialize this object before use? turning off the locking correctness validator. CPU: 12 PID: 753 Comm: mount Tainted: G E 6.7.0-rc6-next-20231222 #504 [...] Call Trace: dump_stack_lvl+0xc5/0x170 dump_stack+0x18/0x30 register_lock_class+0x740/0x7c0 __lock_acquire+0x69/0x13a0 lock_acquire+0x120/0x450 _raw_spin_trylock+0x98/0xd0 ___ratelimit+0xf6/0x220 __ext4_msg+0x7f/0x160 [ext4] ext4_orphan_cleanup+0x665/0x740 [ext4] __ext4_fill_super+0x21ea/0x2b10 [ext4] ext4_fill_super+0x14d/0x360 [ext4] [...] == Normally interval is 0 until s_msg_ratelimit_state is initialized, so ___ratelimit() does nothing. But registering sysfs precedes initializing rs->lock, so it is possible to change rs->interval to a non-zero value via the msg_ratelimit_interval_ms interface of sysfs while rs->lock is uninitialized, and then a call to ext4_msg triggers the problem by accessing an uninitialized rs->lock. Therefore register sysfs after all initializations are complete to avoid such problems.	N/A	More Details
CVE-2024-3799	Insecure handling of POST header parameter body included in requests being sent to an instance of the open-source project Phoniebox allows an attacker to create a website, which – when visited by a user – will send malicious requests to multiple hosts on the local network. If such a request reaches the server, it will cause a shell command execution. This issue affects Phoniebox in all releases through 2.7. Newer 2.x releases were not tested, but they might also be vulnerable. Phoniebox in version 3.0 and higher are not affected.	N/A	More Details
CVE-2024-39505	In the Linux kernel, the following vulnerability has been resolved: drm/komeda: check for error-valued pointer komeda_pipeline_get_state() may return an error-valued pointer, thus check the pointer for negative or null value before dereferencing.	N/A	More Details
CVE-2022-48774	In the Linux kernel, the following vulnerability has been resolved: dmaengine: ptdma: Fix the error handling path in pt_core_init() In order to free resources correctly in the error handling path of pt_core_init(), 2 goto's have to be switched. Otherwise, some resources will leak and we will try to release things that have not been allocated yet. Also move a dev_err() to a place where it is more meaningful.	N/A	More Details
CVE-2024-39507	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash problem in concurrent scenario When link status change, the nic driver need to notify the roce driver to handle this event, but at this time, the roce driver may uninit, then cause kernel crash. To fix the problem, when link status change, need to check whether the roce registered, and when uninit, need to wait link update finish.	N/A	More Details
CVE-2022-48776	In the Linux kernel, the following vulnerability has been resolved: mtd: parsers: qcom: Fix missing free for pparts in cleanup Mtdpart doesn't free pparts when a cleanup function is declared. Add missing free for pparts in cleanup function for smem to fix the leak.	N/A	More Details
CVE-2024-39508	In the Linux kernel, the following vulnerability has been resolved: io_uring/io-wq: Use set_bit() and test_bit() at worker->flags Utilize set_bit() and test_bit() on worker->flags within io_uring/io-wq to address potential data races. The structure io_worker->flags may be accessed through various data paths, leading to concurrency issues. When KCSAN is enabled, it reveals data races occurring in io_worker_handle_work and io_wq_activate_free_worker functions. BUG: KCSAN: data-race in io_worker_handle_work / io_wq_activate_free_worker write to 0xffff8885c4246404 of 4 bytes by task 49071 on cpu 28: io_worker_handle_work (io_uring/io-wq.c:434 io_uring/io-wq.c:569) io_wq_worker (io_uring/io-wq.c:?) <snip> read to 0xffff8885c4246404 of 4 bytes by task 49024 on cpu 5: io_wq_activate_free_worker (io_uring/io-wq.c:? io_uring/io-wq.c:285) io_wq_enqueue (io_uring/io-wq.c:947) io_queue_iowq (io_uring/io_uring.c:524) io_req_task_submit (io_uring/io_uring.c:1511) io_handle_tw_list (io_uring/io_uring.c:1198) <snip> Line numbers against commit 18daea77cca6 ("Merge tag 'for-linus' of git://git.kernel.org/pub/scm/virt/kvm/kvm"). These races involve writes and reads to the same memory location by different tasks running on different CPUs. To mitigate this, refactor the code to use atomic operations such as set_bit(), test_bit(), and clear_bit() instead of basic "and" and "or" operations. This ensures thread-safe manipulation of worker flags. Also, move `create_index` to avoid holes in the structure.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39509	In the Linux kernel, the following vulnerability has been resolved: HID: core: remove unnecessary WARN_ON() in implement() Syzkaller hit a warning [1] in a call to implement() when trying to write a value into a field of smaller size in an output report. Since implement() already has a warn message printed out with the help of hid_warn() and value in question gets trimmed with: ... value &= m; ... WARN_ON may be considered superfluous. Remove it to suppress future syzkaller triggers. [1] WARNING: CPU: 0 PID: 5084 at drivers/hid/hid-core.c:1451 implement drivers/hid/hid-core.c:1451 [inline] WARNING: CPU: 0 PID: 5084 at drivers/hid/hid-core.c:1451 hid_output_report+0x548/0x760 drivers/hid/hid-core.c:1863 Modules linked in: CPU: 0 PID: 5084 Comm: syz-executor424 Not tainted 6.9.0-rc7-syzkaller-00183-gcf87f46fd34d #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/02/2024 RIP: 0010:implement drivers/hid/hid-core.c:1451 [inline] RIP: 0010:hid_output_report+0x548/0x760 drivers/hid/hid-core.c:1863 ... Call Trace: <TASK> __usbhid_submit_report drivers/hid/usbhid/hid-core.c:591 [inline] usbhid_submit_report+0x43d/0x9e0 drivers/hid/usbhid/hid-core.c:636 hiddev_ioctl+0x138b/0x1f00 drivers/hid/usbhid/hiddev.c:726 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:904 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:890 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf5/0x240 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f ...	N/A	More Details
CVE-2022-48780	In the Linux kernel, the following vulnerability has been resolved: net/smc: Avoid overwriting the copies of clcsock callback functions The callback functions of clcsock will be saved and replaced during the fallback. But if the fallback happens more than once, then the copies of these callback functions will be overwritten incorrectly, resulting in a loop call issue: clcsk->sk_error_report l- smc_fback_error_report() <----------l l- smc_fback_forward_wakeup() l (loop) l- clcsock_callback() (incorrectly overwritten) l l- smc->clcsk_error_report() ----------l So this patch fixes the issue by saving these function pointers only once in the fallback and avoiding overwriting.	N/A	More Details
CVE-2024-40900	In the Linux kernel, the following vulnerability has been resolved: cachefiles: remove requests from xarray during flushing requests Even with CACHEFILES_DEAD set, we can still read the requests, so in the following concurrency the request may be used after it has been freed: mount l daemon_thread1 l daemon_thread2 ---------- cachefiles_ondemand_init_object cachefiles_ondemand_send_req REQ_A = kzalloc(sizeof(*req) + data_len) wait_for_completion(&REQ_A->done) cachefiles_daemon_read cachefiles_ondemand_daemon_read // close dev fd cachefiles_flush_reqs complete(&REQ_A->done) kfree(REQ_A) xa_lock(&cache->reqs); cachefiles_ondemand_select_req req->msg.opcode != CACHEFILES_OP_READ // req use-after-free !!! xa_unlock(&cache->reqs); xa_destroy(&cache->reqs) Hence remove requests from cache->reqs when flushing them to avoid accessing freed requests.	N/A	More Details
CVE-2024-40901	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Avoid test/set_bit() operating in non-allocated memory There is a potential out-of-bounds access when using test_bit() on a single word. The test_bit() and set_bit() functions operate on long values, and when testing or setting a single word, they can exceed the word boundary. KASAN detects this issue and produces a dump: BUG: KASAN: slab-out-of-bounds in _scsih_add_device.constprop.0 (./arch/x86/include/asm/bitops.h:60 ./include/asm-generic/bitops/instrumented-atomic.h:29 drivers/scsi/mpt3sas/mpt3sas_scsih.c:7331) mpt3sas Write of size 8 at addr ffff8881d26e3c60 by task kworker/u1536:2/2965 For full log, please look at [1]. Make the allocation at least the size of sizeof(unsigned long) so that set_bit() and test_bit() have sufficient room for read/write operations without overwriting unallocated memory. [1] Link: https://lore.kernel.org/all/ZkNcALr3W3KGYYJG@gmail.com/	N/A	More Details
CVE-2022-48784	In the Linux kernel, the following vulnerability has been resolved: cfg80211: fix race in netlink owner interface destruction My previous fix here to fix the deadlock left a race where the exact same deadlock (see the original commit referenced below) can still happen if cfg80211_destroy_ifaces() already runs while nl80211_netlink_notify() is still marking some interfaces as nl_owner_dead. The race happens because we have two loops here - first we dev_close() all the netdevs, and then we destroy them. If we also have two netdevs (first one need only be a wdev though) then we can find one during the first iteration, close it, and go to the second iteration -- but then find two, and try to destroy also the one we didn't close yet. Fix this by only iterating once.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48785	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: use rcu-safe version of ipv6_get_lladdr() Some time ago 8965779d2c0e ("ipv6,mcast: always hold idev->lock before mca_lock") switched ipv6_get_lladdr() to __ipv6_get_lladdr(), which is rcu-unsafe version. That was OK, because idev->lock was held for these codepaths. In 88e2ca308094 ("mld: convert ifmcaddr6 to RCU") these external locks were removed, so we probably need to restore the original rcu-safe call. Otherwise, we occasionally get a machine crashed/stalled with the following in dmesg: [3405.966610][T230589] general protection fault, probably for non-canonical address 0xdead00000000008c: 0000 [#1] SMP NOPTI [3405.982083][T230589] CPU: 44 PID: 230589 Comm: kworker/44:3 Tainted: G O 5.15.19-cloudflare-2022.2.1 #1 [3405.998061][T230589] Hardware name: SUPA-COOL-SERV [3406.009552][T230589] Workqueue: mld mld_ifc_work [3406.017224][T230589] RIP: 0010:__ipv6_get_lladdr+0x34/0x60 [3406.025780][T230589] Code: 57 10 48 83 c7 08 48 89 e5 48 39 d7 74 3e 48 8d 82 38 ff ff ff eb 13 48 8b 90 d0 00 00 00 48 8d 82 38 ff ff ff 48 39 d7 74 22 <66> 83 78 32 20 77 1b 75 e4 89 ca 23 50 2c 75 dd 48 8b 50 08 48 8b [3406.055748][T230589] RSP: 0018:ffff94e4b3fc3d10 EFLAGS: 00010202 [3406.065617][T230589] RAX: dead00000000005a RBX: ffff94e4b3fc3d30 RCX: 0000000000000040 [3406.077477][T230589] RDX: dead000000000122 RSI: ffff94e4b3fc3d30 RDI: ffff8c3a31431008 [3406.089389][T230589] RBP: ffff94e4b3fc3d10 R08: 0000000000000000 R09: 0000000000000000 [3406.101445][T230589] R10: ffff8c3a31430000 R11: 000000000000000b R12: ffff8c2c37887100 [3406.113553][T230589] R13: ffff8c3a39537000 R14: 00000000000005dc R15: ffff8c3a31431000 [3406.125730][T230589] FS: 0000000000000000(0000) GS:ffff8c3b9fc80000(0000) knlGS:0000000000000000 [3406.138992][T230589] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [3406.149895][T230589] CR2: 00007f0dfea1db60 CR3: 000000387b5f2000 CR4: 0000000000350ee0 [3406.162421][T230589] Call Trace: [3406.170235][T230589] <TASK> [3406.177736][T230589] mld_newpack+0xfe/0x1a0 [3406.186686][T230589] add_grhead+0x87/0xa0 [3406.195498][T230589] add_grec+0x485/0x4e0 [3406.204310][T230589] ? newidle_balance+0x126/0x3f0 [3406.214024][T230589] mld_ifc_work+0x15d/0x450 [3406.223279][T230589] process_one_work+0x1e6/0x380 [3406.232982][T230589] worker_thread+0x50/0x3a0 [3406.242371][T230589] ? rescuer_thread+0x360/0x360 [3406.252175][T230589] kthread+0x127/0x150 [3406.261197][T230589] ? set_kthread_struct+0x40/0x40 [3406.271287][T230589] ret_from_fork+0x22/0x30 [3406.280812][T230589] </TASK> [3406.288937][T230589] Modules linked in: ... [last unloaded: kheaders] [3406.476714][T230589] ---[end trace 3525a7655f2f3b9e]---	N/A	More Details
CVE-2022-48812	In the Linux kernel, the following vulnerability has been resolved: net: dsa: lantiq_gswip: don't use devres for mdiobus As explained in commits: 74b6d7d13307 ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus using devres") mdiobus_free() will panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was not previously unregistered. The GSWIP switch is a platform device, so the initial set of constraints that I thought would cause this (I2C or SPI buses which call ->remove on ->shutdown) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from ->shutdown (like dpaa2-eth, which is on the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumers() will unbind the GSWIP switch driver on shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus allocation and registration, or don't use devres at all. The gswip driver has the code structure in place for orderly mdiobus removal, so just replace devm_mdiobus_alloc() with the non-devres variant, and add manual free where necessary, to ensure that we don't let devres free a still-registered bus.	N/A	More Details
CVE-2022-48813	In the Linux kernel, the following vulnerability has been resolved: net: dsa: felix: don't use devres for mdiobus As explained in commits: 74b6d7d13307 ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus using devres") mdiobus_free() will panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was not previously unregistered. The Felix VSC9959 switch is a PCI device, so the initial set of constraints that I thought would cause this (I2C or SPI buses which call ->remove on ->shutdown) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from ->shutdown (like dpaa2-eth, which is on the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumers() will unbind the felix switch driver on shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus allocation and registration, or don't use devres at all. The felix driver has the code structure in place for orderly mdiobus removal, so just replace devm_mdiobus_alloc_size() with the non-devres variant, and add manual free where necessary, to ensure that we don't let devres free a still-registered bus.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48814	In the Linux kernel, the following vulnerability has been resolved: net: dsa: seville: register the mdiobus under devres As explained in commits: 74b6d7d13307 ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus using devres") mdiobus_free() will panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was not previously unregistered. The Seville VSC9959 switch is a platform device, so the initial set of constraints that I thought would cause this (I2C or SPI buses which call ->remove on ->shutdown) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from ->shutdown (like dpaa2-eth, which is on the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumers() will unbind the seville switch driver on shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus allocation and registration, or don't use devres at all. The seville driver has a code structure that could accommodate both the mdiobus_unregister and mdiobus_free calls, but it has an external dependency upon mscc_miim_setup() from mdio-mscc-miim.c, which calls devm_mdiobus_alloc_size() on its behalf. So rather than restructuring that, and exporting yet one more symbol mscc_miim_teardown(), let's work with devres and replace of_mdiobus_register with the devres variant. When we use all-devres, we can ensure that devres doesn't free a still-registered bus (it either runs both callbacks, or none).	N/A	More Details
CVE-2024-40920	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mst: fix suspicious rcu usage in br_mst_set_state I converted br_mst_set_state to RCU to avoid a vlan use-after-free but forgot to change the vlan group dereference helper. Switch to vlan group RCU deref helper to fix the suspicious rcu usage warning.	N/A	More Details
CVE-2024-40922	In the Linux kernel, the following vulnerability has been resolved: io_uring/rsrc: don't lock while !TASK_RUNNING There is a report of io_rsrc_ref_quiesce() locking a mutex while not TASK_RUNNING, which is due to forgetting restoring the state back after io_run_task_work_sig() and attempts to break out of the waiting loop. do not call blocking ops when !TASK_RUNNING; state=1 set at [<ffffffff815d2494>] prepare_to_wait+0xa4/0x380 kernel/sched/wait.c:237 WARNING: CPU: 2 PID: 397056 at kernel/sched/core.c:10099 __might_sleep+0x114/0x160 kernel/sched/core.c:10099 RIP: 0010:__might_sleep+0x114/0x160 kernel/sched/core.c:10099 Call Trace: <TASK> __mutex_lock_common kernel/locking/mutex.c:585 [inline] __mutex_lock+0xb4/0x940 kernel/locking/mutex.c:752 io_rsrc_ref_quiesce+0x590/0x940 io_uring/rsrc.c:253 io_sqe_buffers_unregister+0xa2/0x340 io_uring/rsrc.c:799 __io_uring_register io_uring/register.c:424 [inline] __do_sys_io_uring_register+0x5b9/0x2400 io_uring/register.c:613 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xd8/0x270 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x6f/0x77	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40923	In the Linux kernel, the following vulnerability has been resolved: vmxnet3: disable rx data ring on dma allocation failure When vmxnet3_rq_create() fails to allocate memory for rq->data_ring.base, the subsequent call to vmxnet3_rq_destroy_all_rxdataring does not reset rq->data_ring.desc_size for the data ring that failed, which presumably causes the hypervisor to reference it on packet reception. To fix this bug, rq->data_ring.desc_size needs to be set to 0 to tell the hypervisor to disable this feature. [95.436876] kernel BUG at net/core/skbuff.c:207! [95.439074] invalid opcode: 0000 [#1] PREEMPT SMP NOPTI [95.440411] CPU: 7 PID: 0 Comm: swapper/7 Not tainted 6.9.3-dirty #1 [95.441558] Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 12/12/2018 [95.443481] RIP: 0010:skb_panic+0x4d/0x4f [95.444404] Code: 4f 70 50 8b 87 c0 00 00 00 50 8b 87 bc 00 00 00 50 ff b7 d0 00 00 00 4c 8b 8f c8 00 00 00 48 c7 c7 68 e8 be 9f e8 63 58 f9 ff <0f> 0b 48 8b 14 24 48 c7 c1 d0 73 65 9f e8 a1 ff ff ff 48 8b 14 24 [95.447684] RSP: 0018:ffffa13340274dd0 EFLAGS: 00010246 [95.448762] RAX: 0000000000000089 RBX: ffff8fbbc72b02d0 RCX: 000000000000083f [95.450148] RDX: 0000000000000000 RSI: 00000000000000f6 RDI: 000000000000083f [95.451520] RBP: 000000000000002d R08: 0000000000000000 R09: ffffa13340274c60 [95.452886] R10: ffffffffa04ed468 R11: 0000000000000002 R12: 0000000000000000 [95.454293] R13: ffff8fbbdab3c2d0 R14: ffff8fbbdbd829e0 R15: ffff8fbbdbd809e0 [95.455682] FS: 0000000000000000(0000) GS:ffff8fbeefd80000(0000) knlGS:0000000000000000 [95.457178] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [95.458340] CR2: 00007fd0d1f650c8 CR3: 0000000115f28000 CR4: 0000000000406f0 [95.459791] Call Trace: [95.460515] <IRQ> [95.461180] ? __die_body.cold+0x19/0x27 [95.462150] ? die+0x2e/0x50 [95.462976] ? do_trap+0xca/0x110 [95.463973] ? do_error_trap+0x6a/0x90 [95.464966] ? skb_panic+0x4d/0x4f [95.465901] ? exc_invalid_op+0x50/0x70 [95.466849] ? skb_panic+0x4d/0x4f [95.467718] ? asm_exc_invalid_op+0x1a/0x20 [95.468758] ? skb_panic+0x4d/0x4f [95.469655] skb_put.cold+0x10/0x10 [95.470573] vmxnet3_rq_rx_complete+0x862/0x11e0 [vmxnet3] [95.471853] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3] [95.473185] __napi_poll+0x2b/0x160 [95.474145] net_rx_action+0x2c6/0x3b0 [95.475115] handle_softirqs+0xe7/0x2a0 [95.476122] __irq_exit_rcu+0x97/0xb0 [95.477109] common_interrupt+0x85/0xa0 [95.478102] </IRQ> [95.478846] <TASK> [95.479603] asm_common_interrupt+0x26/0x40 [95.480657] RIP: 0010:pv_native_safe_halt+0xf/0x20 [95.481801] Code: 22 d7 e9 54 87 01 00 0f 1f 40 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa eb 07 0f 00 2d 93 ba 3b 00 fb f4 <e9> 2c 87 01 00 66 66 2e 0f 1f 84 00 00 00 00 00 90 90 90 90 90 90 [95.485563] RSP: 0018:ffffa133400ffe58 EFLAGS: 00000246 [95.486882] RAX: 0000000000004000 RBX: ffff8fbbc1d14064 RCX: 0000000000000000 [95.488477] RDX: ffff8fbeefd80000 RSI: ffff8fbbc1d14000 RDI: 0000000000000001 [95.490067] RBP: ffff8fbbc1d14064 R08: ffffffffa0652260 R09: 00000000000010d3 [95.491683] R10: 0000000000000018 R11: ffff8fbeefdb4764 R12: ffffffffa0652260 [95.493389] R13: ffffffffa06522e0 R14: 0000000000000001 R15: 0000000000000000 [95.495035] acpi_safe_halt+0x14/0x20 [95.496127] acpi_idle_do_entry+0x2f/0x50 [95.497221] acpi_idle_enter+0x7f/0xd0 [95.498272] cpuidle_enter_state+0x81/0x420 [95.499375] cpuidle_enter+0x2d/0x40 [95.500400] do_idle+0x1e5/0x240 [95.501385] cpu_startup_entry+0x29/0x30 [95.502422] start_secondary+0x11c/0x140 [95.503454] common_startup_64+0x13e/0x141 [95.504466] </TASK> [95.505197] Modules linked in: nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ip ---truncated---	N/A	More Details
CVE-2024-40924	In the Linux kernel, the following vulnerability has been resolved: drm/i915/dpt: Make DPT object unshrinkable In some scenarios, the DPT object gets shrunk but the actual framebuffer did not and thus its still there on the DPT's vm->bound_list. Then it tries to rewrite the PTEs via a stale CPU mapping. This causes panic. [vsyrjala: Add TODO comment] (cherry picked from commit 51064d471c53dcc8eddd2333c3f1c1d9131ba36c)	N/A	More Details
CVE-2024-40925	In the Linux kernel, the following vulnerability has been resolved: block: fix request.queuelist usage in flush Friedrich Weber reported a kernel crash problem and bisected to commit 81ada09cc25e ("blk-flush: reuse rq queuelist in flush state machine"). The root cause is that we use "list_move_tail(&rq->queuelist, pending)" in the PREFLUSH/POSTFLUSH sequences. But rq->queuelist.next == xxx since it's popped out from plug->cached_rq in __blk_mq_alloc_requests_batch(). We don't initialize its queuelist just for this first request, although the queuelist of all later popped requests will be initialized. Fix it by changing to use "list_add_tail(&rq->queuelist, pending)" so rq->queuelist doesn't need to be initialized. It should be ok since rq can't be on any list when PREFLUSH or POSTFLUSH, has no move actually. Please note the commit 81ada09cc25e ("blk-flush: reuse rq queuelist in flush state machine") also has another requirement that no drivers would touch rq->queuelist after blk_mq_end_request() since we will reuse it to add rq to the post-flush pending list in POSTFLUSH. If this is not true, we will have to revert that commit IMHO. This updated version adds "list_del_init(&rq->queuelist)" in flush rq callback since the dm layer may submit request of a weird invalid format (REQ_FSEQ_PREFLUSH | REQ_FSEQ_POSTFLUSH), which causes double list_add if without this "list_del_init(&rq->queuelist)". The weird invalid format problem should be fixed in dm layer.	N/A	More Details
CVE-2024-32753	Under certain circumstances the camera may be susceptible to known vulnerabilities associated with the JQuery versions prior to 3.5.0 third-party component	N/A	More Details
CVE-2024-40926	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: don't attempt to schedule hpd_work on headless cards If the card doesn't have display hardware, hpd_work and hpd_lock are left uninitialized which causes BUG when attempting to schedule hpd_work on runtime PM resume. Fix it by adding headless flag to DRM and skip any hpd if it's set.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40927	In the Linux kernel, the following vulnerability has been resolved: xhci: Handle TD clearing for multiple streams case When multiple streams are in use, multiple TDs might be in flight when an endpoint is stopped. We need to issue a Set TR Dequeue Pointer for each, to ensure everything is reset properly and the caches cleared. Change the logic so that any N>1 TDs found active for different streams are deferred until after the first one is processed, calling xhci_invalidate_cancelled_tds() again from xhci_handle_cmd_set_deq() to queue another command until we are done with all of them. Also change the error/"should never happen" paths to ensure we at least clear any affected TDs, even if we can't issue a command to clear the hardware cache, and complain loudly with an xhci_warn() if this ever happens. This problem case dates back to commit e9df17eb1408 ("USB: xhci: Correct assumptions about number of rings per endpoint.") early on in the XHCI driver's life, when stream support was first added. It was then identified but not fixed nor made into a warning in commit 674f8438c121 ("xhci: split handling halted endpoints into two steps"), which added a FIXME comment for the problem case (without materially changing the behavior as far as I can tell, though the new logic made the problem more obvious). Then later, in commit 94f339147fc3 ("xhci: Fix failure to give back some cached cancelled URBs."), it was acknowledged again. [Mathias: commit 94f339147fc3 ("xhci: Fix failure to give back some cached cancelled URBs.") was a targeted regression fix to the previously mentioned patch. Users reported issues with usb stuck after unmounting/disconnecting UAS devices. This rolled back the TD clearing of multiple streams to its original state.] Apparently the commit author was aware of the problem (yet still chose to submit it): It was still mentioned as a FIXME, an xhci_dbg() was added to log the problem condition, and the remaining issue was mentioned in the commit description. The choice of making the log type xhci_dbg() for what is, at this point, a completely unhandled and known broken condition is puzzling and unfortunate, as it guarantees that no actual users would see the log in production, thereby making it nigh undebuggable (indeed, even if you turn on DEBUG, the message doesn't really hint at there being a problem at all). It took me *months* of random xHC crashes to finally find a reliable repro and be able to do a deep dive debug session, which could all have been avoided had this unhandled, broken condition been actually reported with a warning, as it should have been as a bug intentionally left in unfixed (never mind that it shouldn't have been left in at all). > Another fix to solve clearing the caches of all stream rings with > cancelled TDs is needed, but not as urgent. 3 years after that statement and 14 years after the original bug was introduced, I think it's finally time to fix it. And maybe next time let's not leave bugs unfixed (that are actually worse than the original bug), and let's actually get people to review kernel commits please. Fixes xHC crashes and IOMMU faults with UAS devices when handling errors/faults. Easiest repro is to use `hdparm` to mark an early sector (e.g. 1024) on a disk as bad, then `cat /dev/sdX > /dev/null` in a loop. At least in the case of JMicron controllers, the read errors end up having to cancel two TDs (for two queued requests to different streams) and the one that didn't get cleared properly ends up faulting the xHC entirely when it tries to access DMA pages that have since been unmapped, referred to by the stale TDs. This normally happens quickly (after two or three loops). After this fix, I left the `cat` in a loop running overnight and experienced no xHC failures, with all read errors recovered properly. Repro'd and tested on an Apple M1 Mac Mini (dwc3 host). On systems without an IOMMU, this bug would instead silently corrupt freed memory, making this a ---truncated---	N/A	More Details
CVE-2024-40928	In the Linux kernel, the following vulnerability has been resolved: net: ethtool: fix the error condition in ethtool_get_phy_stats_ethtool() Clang static checker (scan-build) warning: net/ethtool/ioctl.c:line 2233, column 2 Called function pointer is null (null dereference). Return '-EOPNOTSUPP' when 'ops->get_ethtool_phy_stats' is NULL to fix this typo error.	N/A	More Details
CVE-2024-6345	A vulnerability in the package_index module of pypa/setuptools versions up to 69.1.1 allows for remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-controlled inputs, such as package URLs, they can execute arbitrary commands on the system. The issue is fixed in version 70.0.	N/A	More Details
CVE-2024-40929	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: check n_ssids before accessing the ssids In some versions of cfg80211, the ssids poinet might be a valid one even though n_ssids is 0. Accessing the pointer in this case will cuase an out-of-bound access. Fix this by checking n_ssids first.	N/A	More Details
CVE-2024-40930	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: validate HE operation element parsing Validate that the HE operation element has the correct length before parsing it.	N/A	More Details
CVE-2024-40931	In the Linux kernel, the following vulnerability has been resolved: mptcp: ensure snd_una is properly initialized on connect This is strictly related to commit fb7a0d334894 ("mptcp: ensure snd_nxt is properly initialized on connect"). It turns out that syzkaller can trigger the retransmit after fallback and before processing any other incoming packet - so that snd_una is still left uninitialized. Address the issue explicitly initializing snd_una together with snd_nxt and write_seq.	N/A	More Details
CVE-2024-40933	In the Linux kernel, the following vulnerability has been resolved: iio: temperature: mlx90635: Fix ERR_PTR dereference in mlx90635_probe() When devm_regmap_init_i2c() fails, regmap_ee could be error pointer, instead of checking for IS_ERR(regmap_ee), regmap is checked which looks like a copy paste error.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6435	A privilege escalation vulnerability exists in the affected products which could allow a malicious user with basic privileges to access functions which should only be available to users with administrative level privileges. If exploited, an attacker could read sensitive data, and create users. For example, a malicious user with basic privileges could perform critical functions such as creating a user with elevated privileges and reading sensitive information in the “views” section.	N/A	More Details
CVE-2022-45449	Sensitive information disclosure due to excessive privileges assigned to Acronis Agent. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 30984.	N/A	More Details
CVE-2024-40935	In the Linux kernel, the following vulnerability has been resolved: cachefiles: flush all requests after setting CACHEFILES_DEAD In ondemand mode, when the daemon is processing an open request, if the kernel flags the cache as CACHEFILES_DEAD, the cachefiles_daemon_write() will always return -EIO, so the daemon can't pass the copen to the kernel. Then the kernel process that is waiting for the copen triggers a hung_task. Since the DEAD state is irreversible, it can only be exited by closing /dev/cachefiles. Therefore, after calling cachefiles_io_error() to mark the cache as CACHEFILES_DEAD, if in ondemand mode, flush all requests to avoid the above hungtask. We may still be able to read some of the cached data before closing the fd of /dev/cachefiles. Note that this relies on the patch that adds reference counting to the req, otherwise it may UAF.	N/A	More Details
CVE-2024-40936	In the Linux kernel, the following vulnerability has been resolved: cxl/region: Fix memregion leaks in devm_cxl_add_region() Move the mode verification to __create_region() before allocating the memregion to avoid the memregion leaks.	N/A	More Details
CVE-2024-40937	In the Linux kernel, the following vulnerability has been resolved: gve: Clear napi->skb before dev_kfree_skb_any() gve_rx_free_skb incorrectly leaves napi->skb referencing an skb after it is freed with dev_kfree_skb_any(). This can result in a subsequent call to napi_get_frags returning a dangling pointer. Fix this by clearing napi->skb before the skb is freed.	N/A	More Details
CVE-2024-40938	In the Linux kernel, the following vulnerability has been resolved: landlock: Fix d_parent walk The WARN_ON_ONCE() in collect_domain_accesses() can be triggered when trying to link a root mount point. This cannot work in practice because this directory is mounted, but the VFS check is done after the call to security_path_link(). Do not use source directory's d_parent when the source directory is the mount point. [mic: Fix commit message]	N/A	More Details
CVE-2024-40939	In the Linux kernel, the following vulnerability has been resolved: net: wwan: iosm: Fix tainted pointer delete is case of region creation fail In case of region creation fail in ipc_devlink_create_region(), previously created regions delete process starts from tainted pointer which actually holds error code value. Fix this bug by decreasing region index before delete. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2024-5627	The Tournamatch WordPress plugin before 4.6.1 does not sanitise and escape some parameters, which could allow users with a role as low as subscriber to perform Cross-Site Scripting attacks.	N/A	More Details
CVE-2024-40921	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mst: pass vlan group directly to br_mst_vlan_set_state Pass the already obtained vlan group pointer to br_mst_vlan_set_state() instead of dereferencing it again. Each caller has already correctly dereferenced it for their context. This change is required for the following suspicious RCU dereference fix. No functional changes intended.	N/A	More Details
CVE-2024-40919	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Adjust logging of firmware messages in case of released token in __hwrm_send() In case of token is released due to token->state == BNXT_HWRM_DEFERRED, released token (set to NULL) is used in log messages. This issue is expected to be prevented by HWRM_ERR_CODE_PF_UNAVAILABLE error code. But this error code is returned by recent firmware. So some firmware may not return it. This may lead to NULL pointer dereference. Adjust this issue by adding token pointer check. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2022-48815	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: don't use devres for mdiobus As explained in commits: 74b6d7d13307 ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus using devres") mdiobus_free() will panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was not previously unregistered. The Starfighter 2 is a platform device, so the initial set of constraints that I thought would cause this (I2C or SPI buses which call ->remove on ->shutdown) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from ->shutdown (like dpaa2-eth, which is on the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumers() will unbind the bcm_sf2 switch driver on shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus allocation and registration, or don't use devres at all. The bcm_sf2 driver has the code structure in place for orderly mdiobus removal, so just replace devm_mdiobus_alloc() with the non-devres variant, and add manual free where necessary, to ensure that we don't let devres free a still-registered bus.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40918	In the Linux kernel, the following vulnerability has been resolved: parisc: Try to fix random segmentation faults in package builds PA-RISC systems with PA8800 and PA8900 processors have had problems with random segmentation faults for many years. Systems with earlier processors are much more stable. Systems with PA8800 and PA8900 processors have a large L2 cache which needs per page flushing for decent performance when a large range is flushed. The combined cache in these systems is also more sensitive to non-equivalent aliases than the caches in earlier systems. The majority of random segmentation faults that I have looked at appear to be memory corruption in memory allocated using mmap and malloc. My first attempt at fixing the random faults didn't work. On reviewing the cache code, I realized that there were two issues which the existing code didn't handle correctly. Both relate to cache move-in. Another issue is that the present bit in PTEs is racy. 1) PA-RISC caches have a mind of their own and they can speculatively load data and instructions for a page as long as there is a entry in the TLB for the page which allows move-in. TLBs are local to each CPU. Thus, the TLB entry for a page must be purged before flushing the page. This is particularly important on SMP systems. In some of the flush routines, the flush routine would be called and then the TLB entry would be purged. This was because the flush routine needed the TLB entry to do the flush. 2) My initial approach to trying the fix the random faults was to try and use flush_cache_page_if_present for all flush operations. This actually made things worse and led to a couple of hardware lockups. It finally dawned on me that some lines weren't being flushed because the pte check code was racy. This resulted in random inequivalent mappings to physical pages. The __flush_cache_page tmpalias flush sets up its own TLB entry and it doesn't need the existing TLB entry. As long as we can find the pte pointer for the vm page, we can get the pfn and physical address of the page. We can also purge the TLB entry for the page before doing the flush. Further, __flush_cache_page uses a special TLB entry that inhibits cache move-in. When switching page mappings, we need to ensure that lines are removed from the cache. It is not sufficient to just flush the lines to memory as they may come back. This made it clear that we needed to implement all the required flush operations using tmpalias routines. This includes flushes for user and kernel pages. After modifying the code to use tmpalias flushes, it became clear that the random segmentation faults were not fully resolved. The frequency of faults was worse on systems with a 64 MB L2 (PA8900) and systems with more CPUs (rp4440). The warning that I added to flush_cache_page_if_present to detect pages that couldn't be flushed triggered frequently on some systems. Helge and I looked at the pages that couldn't be flushed and found that the PTE was either cleared or for a swap page. Ignoring pages that were swapped out seemed okay but pages with cleared PTEs seemed problematic. I looked at routines related to pte_clear and noticed ptep_clear_flush. The default implementation just flushes the TLB entry. However, it was obvious that on parisc we need to flush the cache page as well. If we don't flush the cache page, stale lines will be left in the cache and cause random corruption. Once a PTE is cleared, there is no way to find the physical address associated with the PTE and flush the associated page at a later time. I implemented an updated change with a parisc specific version of ptep_clear_flush. It fixed the random data corruption on Helge's rp4440 and rp3440, as well as on my c8000. At this point, I realized that I could restore the code where we only flush in flush_cache_page_if_present if the page has been accessed. However, for this, we also need to flush the cache when the accessed bit is cleared in ---truncated---	N/A	More Details
CVE-2022-48816	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: lock against ->sock changing during sysfs read ->sock can be set to NULL asynchronously unless ->recv_mutex is held. So it is important to hold that mutex. Otherwise a sysfs read can trigger an oops. Commit 17f09d3f619a ("SUNRPC: Check if the xprt is connected before handling sysfs reads") appears to attempt to fix this problem, but it only narrows the race window.	N/A	More Details
CVE-2022-48817	In the Linux kernel, the following vulnerability has been resolved: net: dsa: ar9331: register the mdiobus under devres As explained in commits: 74b6d7d13307 ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus using devres") mdiobus_free() will panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was not previously unregistered. The ar9331 is an MDIO device, so the initial set of constraints that I thought would cause this (I2C or SPI buses which call ->remove on ->shutdown) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from ->shutdown (like dpaa2-eth, which is on the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumers() will unbind the ar9331 switch driver on shutdown. So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus allocation and registration, or don't use devres at all. The ar9331 driver doesn't have a complex code structure for mdiobus removal, so just replace of_mdiobus_register with the devres variant in order to be all-devres and ensure that we don't free a still-registered bus.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48818	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: don't use devres for mdiobus As explained in commits: 74b6d7d13307 ("net: dsa: realtek: register the MDIO bus under devres") 5135e96a3dd2 ("net: dsa: don't allocate the slave_mii_bus using devres") mdiobus_free() will panic when called from devm_mdiobus_free() <- devres_release_all() <- __device_release_driver(), and that mdiobus was not previously unregistered. The mv88e6xxx is an MDIO device, so the initial set of constraints that I thought would cause this (I2C or SPI buses which call ->remove on ->shutdown) do not apply. But there is one more which applies here. If the DSA master itself is on a bus that calls ->remove from ->shutdown (like dpaa2-eth, which is on the fsl-mc bus), there is a device link between the switch and the DSA master, and device_links_unbind_consumers() will unbind the Marvell switch driver on shutdown. systemd-shutdown[1]: Powering off. mv88e6085 0x0000000008b96000:00 sw_gl0: Link is Down fsl-mc dpbp.9: Removing from iommu group 7 fsl-mc dpbp.8: Removing from iommu group 7 ----------[cut here]---------- kernel BUG at drivers/net/phy/mdio_bus.c:677! Internal error: Oops - BUG: 0 [#1] PREEMPT SMP Modules linked in: CPU: 0 PID: 1 Comm: systemd-shutdow Not tainted 5.16.5-00040-gdc05f73788e5 #15 pc : mdiobus_free+0x44/0x50 lr : devm_mdiobus_free+0x10/0x20 Call trace: mdiobus_free+0x44/0x50 devm_mdiobus_free+0x10/0x20 devres_release_all+0xa0/0x100 __device_release_driver+0x190/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumers+0xd4/0x100 __device_release_driver+0x4c/0x220 device_release_driver_internal+0xac/0xb0 device_links_unbind_consumers+0xd4/0x100 __device_release_driver+0x94/0x220 device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_device_remove+0x24/0x40 __fsl_mc_device_remove+0xc/0x20 device_for_each_child+0x58/0xa0 dprc_remove+0x90/0xb0 fsl_mc_driver_remove+0x20/0x5c __device_release_driver+0x21c/0x220 device_release_driver+0x28/0x40 bus_remove_device+0x118/0x124 device_del+0x174/0x420 fsl_mc_bus_remove+0x80/0x100 fsl_mc_bus_shutdown+0xc/0x1c platform_shutdown+0x20/0x30 device_shutdown+0x154/0x330 kernel_power_off+0x34/0x6c __do_sys_reboot+0x15c/0x250 __arm64_sys_reboot+0x20/0x30 invoke_syscall.constprop.0+0x4c/0xe0 do_el0_svc+0x4c/0x150 el0_svc+0x24/0xb0 el0t_64_sync_handler+0xa8/0xb0 el0t_64_sync+0x178/0x17c So the same treatment must be applied to all DSA switch drivers, which is: either use devres for both the mdiobus allocation and registration, or don't use devres at all. The Marvell driver already has a good structure for mdiobus removal, so just plug in mdiobus_free and get rid of devres.	N/A	More Details
CVE-2022-48819	In the Linux kernel, the following vulnerability has been resolved: tcp: take care of mixed splice()/sendmsg(MSG_ZEROCOPY) case syzbot found that mixing sendpage() and sendmsg(MSG_ZEROCOPY) calls over the same TCP socket would again trigger the infamous warning in inet_sock_destruct() WARN_ON(sk_forward_alloc_get(sk)); While Talal took into account a mix of regular copied data and MSG_ZEROCOPY one in the same skb, the sendpage() path has been forgotten. We want the charging to happen for sendpage(), because pages could be coming from a pipe. What is missing is the downgrading of pure zerocopy status to make sure sk_forward_alloc will stay synced. Add tcp_downgrade_zcopy_pure() helper so that we can use it from the two callers.	N/A	More Details
CVE-2022-48821	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: avoid double fput() on failed usercopy If the copy back to userland fails for the FASTRPC_IOCTL_ALLOC_DMA_BUFF ioctl(), we shouldn't assume that 'buf->dmabuf' is still valid. In fact, dma_buf_fd() called fd_install() before, i.e. "consumed" one reference, leaving us with none. Calling dma_buf_put() will therefore put a reference we no longer own, leading to a valid file descritor table entry for an already released 'file' object which is a straight use-after-free. Simply avoid calling dma_buf_put() and rely on the process exit code to do the necessary cleanup, if needed, i.e. if the file descriptor is still valid.	N/A	More Details
CVE-2024-6396	A vulnerability in the `_backup_run` function in aimhubio/aim version 3.19.3 allows remote attackers to overwrite any file on the host server and exfiltrate arbitrary data. The vulnerability arises due to improper handling of the `run_hash` and `repo.path` parameters, which can be manipulated to create and write to arbitrary file paths. This can lead to denial of service by overwriting critical system files, loss of private data, and potential remote code execution.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48823	In the Linux kernel, the following vulnerability has been resolved: scsi: qedf: Fix refcount issue when LOGO is received during TMF Hung task call trace was seen during LOGO processing. [974.309060] [0000:00:00.0]: [qedf_eh_device_reset:868]: 1:0:2:0: LUN RESET Issued... [974.309065] [0000:00:00.0]:[qedf_initiate_tmf:2422]: tm_flags 0x10 sc_cmd 00000000c16b930f op = 0x2a target_id = 0x2 lun=0 [974.309178] [0000:00:00.0]: [qedf_initiate_tmf:2431]: portid=016900 tm_flags =LUN RESET [974.309222] [0000:00:00.0]:[qedf_initiate_tmf:2438]: orig io_req = 00000000ec78df8f xid = 0x180 ref_cnt = 1. [974.309625] host1: rport 016900: Received LOGO request while in state Ready [974.309627] host1: rport 016900: Delete port [974.309642] host1: rport 016900: work event 3 [974.309644] host1: rport 016900: lld callback ev 3 [974.313243] [0000:61:00.2]:[qedf_execute_tmf:2383]:1: fcport is uploading, not executing flush. [974.313295] [0000:61:00.2]:[qedf_execute_tmf:2400]:1: task mgmt command success... [984.031088] INFO: task jbd2/dm-15-8:7645 blocked for more than 120 seconds. [984.031136] Not tainted 4.18.0-305.el8.x86_64 #1 [984.031166] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. [984.031209] jbd2/dm-15-8 D 0 7645 2 0x80004080 [984.031212] Call Trace: [984.031222] __schedule+0x2c4/0x700 [984.031230] ? unfreeze_partials.isra.83+0x16e/0x1a0 [984.031233] ? bit_wait_timeout+0x90/0x90 [984.031235] schedule+0x38/0xa0 [984.031238] io_schedule+0x12/0x40 [984.031240] bit_wait_io+0xd/0x50 [984.031243] __wait_on_bit+0x6c/0x80 [984.031248] ? free_buffer_head+0x21/0x50 [984.031251] out_of_line_wait_on_bit+0x91/0xb0 [984.031257] ? init_wait_var_entry+0x50/0x50 [984.031268] jbd2_journal_commit_transaction+0x112e/0x19f0 [jbd2] [984.031280] kjournald2+0xbd/0x270 [jbd2] [984.031284] ? finish_wait+0x80/0x80 [984.031291] ? commit_timeout+0x10/0x10 [jbd2] [984.031294] kthread+0x116/0x130 [984.031300] ? kthread_flush_work_fn+0x10/0x10 [984.031305] ret_from_fork+0x1f/0x40 There was a ref count issue when LOGO is received during TMF. This leads to one of the I/Os hanging with the driver. Fix the ref count.	N/A	More Details
CVE-2024-6721	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. Consult IDs: CVE-2024-5324. Reason: This record is a reservation duplicate of CVE-2024-5324. Notes: All CVE users should reference CVE-2024-5324 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-48825	In the Linux kernel, the following vulnerability has been resolved: scsi: qedf: Add stag_work to all the vports Call trace seen when creating NPIV ports, only 32 out of 64 show online. stag work was not initialized for vport, hence initialize the stag work. WARNING: CPU: 8 PID: 645 at kernel/workqueue.c:1635 __queue_delayed_work+0x68/0x80 CPU: 8 PID: 645 Comm: kworker/8:1 Kdump: loaded Tainted: G IOE --------- -- 4.18.0-348.el8.x86_64 #1 Hardware name: Dell Inc. PowerEdge MX740c/0177V9, BIOS 2.12.2 07/09/2021 Workqueue: events fc_lport_timeout [libfc] RIP: 0010:__queue_delayed_work+0x68/0x80 Code: 89 b2 88 00 00 00 44 89 82 90 00 00 00 48 01 c8 48 89 42 50 41 81 f8 00 20 00 00 75 1d e9 60 24 07 00 44 89 c7 e9 98 f6 ff ff <0f> 0b eb c5 0f 0b eb a1 0f 0b eb a7 0f 0b eb ac 44 89 c6 e9 40 23 RSP: 0018:ffffae514bc3be40 EFLAGS: 00010006 RAX: ffff8d25d6143750 RBX: 0000000000000202 RCX: 0000000000000002 RDX: ffff8d2e31383748 RSI: ffff8d25c000d600 RDI: ffff8d2e31383788 RBP: ffff8d2e31380de0 R08: 0000000000002000 R09: ffff8d2e31383750 R10: ffffffffc0c957e0 R11: ffff8d2624800000 R12: ffff8d2e31380a58 R13: ffff8d2d915eb000 R14: ffff8d25c499b5c0 R15: ffff8d2e31380e18 FS: 0000000000000000(0000) GS:ffff8d2d1fb00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055fd0484b8b8 CR3: 00000008ffc10006 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: queue_delayed_work_on+0x36/0x40 qedf_elsct_send+0x57/0x60 [qedf] fc_lport_enter_flogi+0x90/0xc0 [libfc] fc_lport_timeout+0xb7/0x140 [libfc] process_one_work+0x1a7/0x360 ? create_worker+0x1a0/0x1a0 worker_thread+0x30/0x390 ? create_worker+0x1a0/0x1a0 kthread+0x116/0x130 ? kthread_flush_work_fn+0x10/0x10 ret_from_fork+0x35/0x40 ---[end trace 008f00f722f2c2ff]-- Initialize stag work for all the vports.	N/A	More Details
CVE-2022-48827	In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix the behavior of READ near OFFSET_MAX Dan Aloni reports: > Due to commit 8cfb9015280d ("NFS: Always provide aligned buffers to > the RPC read layers") on the client, a read of 0xfff is aligned up > to server rsize of 0x1000. > > As a result, in a test where the server has a file of size > 0x7fffffffffffffff, and the client tries to read from the offset > 0x7ffffffffffff000, the read causes loff_t overflow in the server > and it returns an NFS code of EINVAL to the client. The client as > a result indefinitely retries the request. The Linux NFS client does not handle NFS?ERR_INVAL, even though all NFS specifications permit servers to return that status code for a READ. Instead of NFS?ERR_INVAL, have out-of-range READ requests succeed and return a short result. Set the EOF flag in the result to prevent the client from retrying the READ request. This behavior appears to be consistent with Solaris NFS servers. Note that NFSv3 and NFSv4 use u64 offset values on the wire. These must be converted to loff_t internally before use -- an implicit type cast is not adequate for this purpose. Otherwise VFS checks against sb->s_maxbytes do not work properly.	N/A	More Details
CVE-2022-48828	In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix ia_size underflow iattr::ia_size is a loff_t, which is a signed 64-bit type. NFSv3 and NFSv4 both define file size as an unsigned 64-bit type. Thus there is a range of valid file size values an NFS client can send that is already larger than Linux can handle. Currently decode_fattr4() dumps a full u64 value into ia_size. If that value happens to be larger than S64_MAX, then ia_size underflows. I'm about to fix up the NFSv3 behavior as well, so let's catch the underflow in the common code path: nfsd_setattr().	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48829	In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix NFSv3 SETATTR/CREATE's handling of large file sizes iattr::ia_size is a loff_t, so these NFSv3 procedures must be careful to deal with incoming client size values that are larger than s64_max without corrupting the value. Silently capping the value results in storing a different value than the client passed in which is unexpected behavior, so remove the min_t() check in decode_sattr3(). Note that RFC 1813 permits only the WRITE procedure to return NFS3ERR_FBIG. We believe that NFSv3 reference implementations also return NFS3ERR_FBIG when ia_size is too large.	N/A	More Details
CVE-2022-48830	In the Linux kernel, the following vulnerability has been resolved: can: isotp: fix potential CAN frame reception race in isotp_rcv() When receiving a CAN frame the current code logic does not consider concurrently receiving processes which do not show up in real world usage. Ziyang Xuan writes: The following syz problem is one of the scenarios. so->rx.len is changed by isotp_rcv_ff() during isotp_rcv_cf(), so->rx.len equals 0 before alloc_skb() and equals 4096 after alloc_skb(). That will trigger skb_over_panic() in skb_put(). ========== CPU: 1 PID: 19 Comm: ksoftirqd/1 Not tainted 5.16.0-rc8-syzkaller #0 RIP: 0010:skb_panic+0x16c/0x16e net/core/skbuff.c:113 Call Trace: <TASK> skb_over_panic net/core/skbuff.c:118 [inline] skb_put.cold+0x24/0x24 net/core/skbuff.c:1990 isotp_rcv_cf net/can/isotp.c:570 [inline] isotp_rcv+0xa38/0x1e30 net/can/isotp.c:668 deliver net/can/af_can.c:574 [inline] can_rcv_filter+0x445/0x8d0 net/can/af_can.c:635 can_receive+0x31d/0x580 net/can/af_can.c:665 can_rcv+0x120/0x1c0 net/can/af_can.c:696 __netif_receive_skb_one_core+0x114/0x180 net/core/dev.c:5465 __netif_receive_skb+0x24/0x1b0 net/core/dev.c:5579 Therefore we make sure the state changes and data structures stay consistent at CAN frame reception time by adding a spin_lock in isotp_rcv(). This fixes the issue reported by syzkaller but does not affect real world operation.	N/A	More Details
CVE-2022-48831	In the Linux kernel, the following vulnerability has been resolved: ima: fix reference leak in asymmetric_verify() Don't leak a reference to the key if its algorithm is unknown.	N/A	More Details
CVE-2022-48832	In the Linux kernel, the following vulnerability has been resolved: audit: don't deref the syscall args when checking the openat2 open_how::flags As reported by Jeff, dereferencing the openat2 syscall argument in audit_match_perm() to obtain the open_how::flags can result in an oops/page-fault. This patch fixes this by using the open_how struct that we store in the audit_context with audit_openat2_how(). Independent of this patch, Richard Guy Briggs posted a similar patch to the audit mailing list roughly 40 minutes after this patch was posted.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48833	In the Linux kernel, the following vulnerability has been resolved: btrfs: skip reserved bytes warning on unmount after log cleanup failure After the recent changes made by commit c2e39305299f01 ("btrfs: clear extent buffer uptodate when we fail to write it") and its followup fix, commit 651740a5024117 ("btrfs: check WRITE_ERR when trying to read an extent buffer"), we can now end up not cleaning up space reservations of log tree extent buffers after a transaction abort happens, as well as not cleaning up still dirty extent buffers. This happens because if writeback for a log tree extent buffer failed, then we have cleared the bit EXTENT_BUFFER_UPTODATE from the extent buffer and we have also set the bit EXTENT_BUFFER_WRITE_ERR on it. Later on, when trying to free the log tree with free_log_tree(), which iterates over the tree, we can end up getting an -EIO error when trying to read a node or a leaf, since read_extent_buffer_pages() returns -EIO if an extent buffer does not have EXTENT_BUFFER_UPTODATE set and has the EXTENT_BUFFER_WRITE_ERR bit set. Getting that -EIO means that we return immediately as we can not iterate over the entire tree. In that case we never update the reserved space for an extent buffer in the respective block group and space_info object. When this happens we get the following traces when unmounting the fs: [174957.284509] BTRFS: error (device dm-0) in cleanup_transaction:1913: errno=-5 IO failure [174957.286497] BTRFS: error (device dm-0) in free_log_tree:3420: errno=-5 IO failure [174957.399379] ------------[cut here]------------ [174957.402497] WARNING: CPU: 2 PID: 3206883 at fs/btrfs/block-group.c:127 btrfs_put_block_group+0x77/0xb0 [btrfs] [174957.407523] Modules linked in: btrfs overlay dm_zero (...) [174957.424917] CPU: 2 PID: 3206883 Comm: umount Tainted: G W 5.16.0-rc5-btrfs-next-109 #1 [174957.426689] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org 04/01/2014 [174957.428716] RIP: 0010:btrfs_put_block_group+0x77/0xb0 [btrfs] [174957.429717] Code: 21 48 8b bd (...) [174957.432867] RSP: 0018:ffffb70d41cffdd0 EFLAGS: 00010206 [174957.433632] RAX: 0000000000000001 RBX: ffff8b09c3848000 RCX: ffff8b0758edd1c8 [174957.434689] RDX: 0000000000000001 RSI: ffffffffc0b467e7 RDI: ffff8b0758edd000 [174957.436068] RBP: ffff8b0758edd000 R08: 0000000000000000 R09: 0000000000000000 [174957.437114] R10: 0000000000000246 R11: 0000000000000000 R12: ffff8b09c3848148 [174957.438140] R13: ffff8b09c3848198 R14: ffff8b0758edd188 R15: dead000000000100 [174957.439317] FS: 00007f328fb82800(0000) GS:ffff8b0a2d200000(0000) knlGS:0000000000000000 [174957.440402] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [174957.441164] CR2: 00007fff13563e98 CR3: 0000000404f4e005 CR4: 0000000000370ee0 [174957.442117] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [174957.443076] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [174957.443948] Call Trace: [174957.444264] <TASK> [174957.444538] btrfs_free_block_groups+0x255/0x3c0 [btrfs] [174957.445238] close_ctree+0x301/0x357 [btrfs] [174957.445803] ? call_rcu+0x16c/0x290 [174957.446250] generic_shutdown_super+0x74/0x120 [174957.446832] kill_anon_super+0x14/0x30 [174957.447305] btrfs_kill_super+0x12/0x20 [btrfs] [174957.447890] deactivate_locked_super+0x31/0xa0 [174957.448440] cleanup_mnt+0x147/0x1c0 [174957.448888] task_work_run+0x5c/0xa0 [174957.449336] exit_to_user_mode_prepare+0x1e5/0x1f0 [174957.449934] syscall_exit_to_user_mode+0x16/0x40 [174957.450512] do_syscall_64+0x48/0xc0 [174957.450980] entry_SYSCALL_64_after_hwframe+0x44/0xae [174957.451605] RIP: 0033:0x7f328fdc4a97 [174957.452059] Code: 03 0c 00 f7 (...) [174957.454320] RSP: 002b:00007fff13564ec8 EFLAGS: 00000246 ORIG_RAX: 00000000000000a6 [174957.455262] RAX: 0000000000000000 RBX: 00007f328feea264 RCX: 00007f328fdc4a97 [174957.456131] RDX: 0000000000000000 RSI: 00000000000000 ---truncated---	N/A	More Details
CVE-2024-40913	In the Linux kernel, the following vulnerability has been resolved: cachefiles: defer exposing anon_fd until after copy_to_user() succeeds After installing the anonymous fd, we can now see it in userland and close it. However, at this point we may not have gotten the reference count of the cache, but we will put it during colse fd, so this may cause a cache UAF. So grab the cache reference count before fd_install(). In addition, by kernel convention, fd is taken over by the user land after fd_install(), and the kernel should not call close_fd() after that, i.e., it should call fd_install() after everything is ready, thus fd_install() is called after copy_to_user() succeeds.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40914	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: don't unpoison huge_zero_folio When I did memory failure tests recently, below panic occurs: kernel BUG at include/linux/mm.h:1135! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 9 PID: 137 Comm: kswapd1 Not tainted 6.9.0-rc4-00491-gd5ce28f156fe-dirty #14 RIP: 0010:shrink_huge_zero_page_scan+0x168/0x1a0 RSP: 0018:ffff9933c6c57bd0 EFLAGS: 00000246 RAX: 000000000000003e RBX: 0000000000000000 RCX: ffff88f61fc5c9c8 RDX: 0000000000000000 RSI: 0000000000000027 RDI: ffff88f61fc5c9c0 RBP: ffffcd7c446b0000 R08: ffffffff9a9405f0 R09: 0000000000005492 R10: 00000000000030ea R11: ffffffff9a9405f0 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ffff88e703c4ac00 FS: 0000000000000000(0000) GS:ffff88f61fc40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055f4da6e9878 CR3: 0000000c71048000 CR4: 00000000000006f0 Call Trace: <TASK> do_shrink_slab+0x14f/0x6a0 shrink_slab+0xca/0x8c0 shrink_node+0x2d0/0x7d0 balance_pgdat+0x33a/0x720 kswapd+0x1f3/0x410 kthread+0xd5/0x100 ret_from_fork+0x2f/0x50 ret_from_fork_asm+0x1a/0x30 </TASK> Modules linked in: mce_inject hwpoison_inject ---[end trace 0000000000000000]--- RIP: 0010:shrink_huge_zero_page_scan+0x168/0x1a0 RSP: 0018:ffff9933c6c57bd0 EFLAGS: 00000246 RAX: 000000000000003e RBX: 0000000000000000 RCX: ffff88f61fc5c9c8 RDX: 0000000000000000 RSI: 0000000000000027 RDI: ffff88f61fc5c9c0 RBP: ffffcd7c446b0000 R08: ffffffff9a9405f0 R09: 0000000000005492 R10: 00000000000030ea R11: ffffffff9a9405f0 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ffff88e703c4ac00 FS: 0000000000000000(0000) GS:ffff88f61fc40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055f4da6e9878 CR3: 0000000c71048000 CR4: 00000000000006f0 The root cause is that HWPoison flag will be set for huge_zero_folio without increasing the folio refcnt. But then unpoison_memory() will decrease the folio refcnt unexpectedly as it appears like a successfully hwpoisoned folio leading to VM_BUG_ON_PAGE(page_ref_count(page) == 0) when releasing huge_zero_folio. Skip unpoisoning huge_zero_folio in unpoison_memory() to fix this issue. We're not prepared to unpoison huge_zero_folio yet.	N/A	More Details
CVE-2024-40915	In the Linux kernel, the following vulnerability has been resolved: riscv: rewrite __kernel_map_pages() to fix sleeping in invalid context __kernel_map_pages() is a debug function which clears the valid bit in page table entry for deallocated pages to detect illegal memory accesses to freed pages. This function set/clear the valid bit using __set_memory(). __set_memory() acquires init_mm's semaphore, and this operation may sleep. This is problematic, because __kernel_map_pages() can be called in atomic context, and thus is illegal to sleep. An example warning that this causes: BUG: sleeping function called from invalid context at kernel/locking/rwsem.c:1578 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 2, name: kthreadd preempt_count: 2, expected: 0 CPU: 0 PID: 2 Comm: kthreadd Not tainted 6.9.0-g1d4c6d784ef6 #37 Hardware name: riscv-virtio,qemu (DT) Call Trace: [<ffffffff800060dc>] dump_backtrace+0x1c/0x24 [<ffffffff8091ef6e>] show_stack+0x2c/0x38 [<ffffffff8092baf8>] dump_stack_lvl+0x5a/0x72 [<ffffffff8092bb24>] dump_stack+0x14/0x1c [<ffffffff8003b7ac>] __might_resched+0x104/0x10e [<ffffffff8003b7f4>] __might_sleep+0x3e/0x62 [<ffffffff8093276a>] down_write+0x20/0x72 [<ffffffff8000cf00>] __set_memory+0x82/0x2fa [<ffffffff8000d324>] __kernel_map_pages+0x5a/0xd4 [<ffffffff80196cca>] __alloc_pages_bulk+0x3b2/0x43a [<ffffffff8018ee82>] __vmalloc_node_range+0x196/0x6ba [<ffffffff80011904>] copy_process+0x72c/0x17ec [<ffffffff80012ab4>] kernel_clone+0x60/0x2fe [<ffffffff80012f62>] kernel_thread+0x82/0xa0 [<ffffffff8003552c>] kthreadd+0x14a/0x1be [<ffffffff809357de>] ret_from_fork+0xe/0x1c Rewrite this function with apply_to_existing_page_range(). It is fine to not have any locking, because __kernel_map_pages() works with pages being allocated/deallocated and those pages are not changed by anyone else in the meantime.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40916	In the Linux kernel, the following vulnerability has been resolved: drm/exynos: hdmi: report safe 640x480 mode as a fallback when no EDID found When reading EDID fails and driver reports no modes available, the DRM core adds an artificial 1024x786 mode to the connector. Unfortunately some variants of the Exynos HDMI (like the one in Exynos4 SoCs) are not able to drive such mode, so report a safe 640x480 mode instead of nothing in case of the EDID reading failure. This fixes the following issue observed on Trats2 board since commit 13d5b040363c ("drm/exynos: do not return negative values from .get_modes()"): [drm] Exynos DRM: using 11c00000.fimd device for DMA mapping operations exynos-drm exynos-drm: bound 11c00000.fimd (ops fimd_component_ops) exynos-drm exynos-drm: bound 12c10000.mixer (ops mixer_component_ops) exynos-dsi 11c80000.dsi: [drm:samsung_dsim_host_attach] Attached s6e8aa0 device (lanes:4 bpp:24 mode-flags:0x10b) exynos-drm exynos-drm: bound 11c80000.dsi (ops exynos_dsi_component_ops) exynos-drm exynos-drm: bound 12d00000.hdmi (ops hdmi_component_ops) [drm] Initialized exynos 1.1.0 20180330 for exynos-drm on minor 1 exynos-hdmi 12d00000.hdmi: [drm:hdmiphy_enable.part.0] *ERROR* PLL could not reach steady state panel-samsung-s6e8aa0 11c80000.dsi.0: ID: 0xa2, 0x20, 0x8c exynos-mixer 12c10000.mixer: timeout waiting for VSYNC ------------[cut here]------------ WARNING: CPU: 1 PID: 11 at drivers/gpu/drm/drm_atomic_helper.c:1682 drm_atomic_helper_wait_for_vblanks.part.0+0x2b0/0x2b8 [CRTC:70:crtc-1] vblank wait timed out Modules linked in: CPU: 1 PID: 11 Comm: kworker/u16:0 Not tainted 6.9.0-rc5-next-20240424 #14913 Hardware name: Samsung Exynos (Flattened Device Tree) Workqueue: events_unbound deferred_probe_work_func Call trace: unwind_backtrace from show_stack+0x10/0x14 show_stack from dump_stack_lvl+0x68/0x88 dump_stack_lvl from __warn+0x7c/0x1c4 __warn from warn_slowpath_fmt+0x11c/0x1a8 warn_slowpath_fmt from drm_atomic_helper_wait_for_vblanks.part.0+0x2b0/0x2b8 drm_atomic_helper_wait_for_vblanks.part.0 from drm_atomic_helper_commit_tail_rpm+0x7c/0x8c drm_atomic_helper_commit_tail_rpm from commit_tail+0x9c/0x184 commit_tail from drm_atomic_helper_commit+0x168/0x190 drm_atomic_helper_commit from drm_atomic_commit+0xb4/0xe0 drm_atomic_commit from drm_client_modeset_commit_atomic+0x23c/0x27c drm_client_modeset_commit_atomic from drm_client_modeset_commit_locked+0x60/0x1cc drm_client_modeset_commit_locked from drm_client_modeset_commit+0x24/0x40 drm_client_modeset_commit from __drm_fb_helper_restore_fbdev_mode_unlocked+0x9c/0xc4 __drm_fb_helper_restore_fbdev_mode_unlocked from drm_fb_helper_set_par+0x2c/0x3c drm_fb_helper_set_par from fbcon_init+0x3d8/0x550 fbcon_init from visual_init+0xc0/0x108 visual_init from do_bind_con_driver+0x1b8/0x3a4 do_bind_con_driver from do_take_over_console+0x140/0x1ec do_take_over_console from do_fbcon_takeover+0x70/0xd0 do_fbcon_takeover from fbcon_fb_registered+0x19c/0x1ac fbcon_fb_registered from register_framebuffer+0x190/0x21c register_framebuffer from __drm_fb_helper_initial_config_and_unlock+0x350/0x574 __drm_fb_helper_initial_config_and_unlock from exynos_drm_fbdev_client_hotplug+0x6c/0xb0 exynos_drm_fbdev_client_hotplug from drm_client_register+0x58/0x94 drm_client_register from exynos_drm_bind+0x160/0x190 exynos_drm_bind from try_to_bring_up_aggregate_device+0x200/0x2d8 try_to_bring_up_aggregate_device from __component_add+0xb0/0x170 __component_add from mixer_probe+0x74/0xcc mixer_probe from platform_probe+0x5c/0xb8 platform_probe from really_probe+0xe0/0x3d8 really_probe from __driver_probe_device+0x9c/0x1e4 __driver_probe_device from driver_probe_device+0x30/0xc0 driver_probe_device from __device_attach_driver+0xa8/0x120 __device_attach_driver from bus_for_each_drv+0x80/0xcc bus_for_each_drv from __device_attach+0xac/0x1fc __device_attach from bus_probe_device+0x8c/0x90 bus_probe_device from deferred_probe_work_func+0 ---truncated---	N/A	More Details
CVE-2024-40917	In the Linux kernel, the following vulnerability has been resolved: memblock: make memblock_set_node() also warn about use of MAX_NUMNODES On an (old) x86 system with SRAT just covering space above 4Gb: ACPI: SRAT: Node 0 PXM 0 [mem 0x100000000-0xfffffffff] hotplug the commit referenced below leads to this NUMA configuration no longer being refused by a CONFIG_NUMA=y kernel (previously NUMA: nodes only cover 6144MB of your 8185MB e820 RAM. Not used. No NUMA configuration found Faking a node at [mem 0x0000000000000000-0x000000027fffffff] was seen in the log directly after the message quoted above), because of memblock_validate_numa_coverage() checking for NUMA_NO_NODE (only). This in turn led to memblock_alloc_range_nid()'s warning about MAX_NUMNODES triggering, followed by a NULL deref in memmap_init() when trying to access node 64's (NODE_SHIFT=6) node data. To compensate said change, make memblock_set_node() warn on and adjust a passed in value of MAX_NUMNODES, just like various other functions already do.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47623	In the Linux kernel, the following vulnerability has been resolved: powerpc/fixmap: Fix VM debug warning on unmap Unmapping a fixmap entry is done by calling __set_fixmap() with FIXMAP_PAGE_CLEAR as flags. Today, powerpc __set_fixmap() calls map_kernel_page(). map_kernel_page() is not happy when called a second time for the same page. WARNING: CPU: 0 PID: 1 at arch/powerpc/mm/pgtable.c:194 set_pte_at+0xc/0x1e8 CPU: 0 PID: 1 Comm: swapper Not tainted 5.16.0-rc3-s3k-dev-01993-g350ff07feb7d-dirty #682 NIP: c0017cd4 LR: c00187f0 CTR: 00000010 REGS: e1011d50 TRAP: 0700 Not tainted (5.16.0-rc3-s3k-dev-01993-g350ff07feb7d-dirty) MSR: 00029032 <EE,ME,IR,DR,RI> CR: 42000208 XER: 00000000 GPR00: c0165fec e1011e10 c14c0000 c0ee2550 ff800000 c0f3d000 00000000 c001686c GPR08: 00001000 b00045a9 00000001 c0f58460 c0f50000 00000000 c0007e10 00000000 GPR16: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 GPR24: 00000000 00000000 c0ee2550 00000000 c0f57000 00000ff8 00000000 ff800000 NIP [c0017cd4] set_pte_at+0xc/0x1e8 LR [c00187f0] map_kernel_page+0x9c/0x100 Call Trace: [e1011e10] [c0736c68] vsnprintf+0x358/0x6c8 (unreliable) [e1011e30] [c0165fec] __set_fixmap+0x30/0x44 [e1011e40] [c0c13bdc] early_iounmap+0x11c/0x170 [e1011e70] [c0c06cb0] ioremap_legacy_serial_console+0x88/0xc0 [e1011e90] [c0c03634] do_one_initcall+0x80/0x178 [e1011ef0] [c0c0385c] kernel_init_freeable+0xb4/0x250 [e1011f20] [c0007e34] kernel_init+0x24/0x140 [e1011f30] [c0016268] ret_from_kernel_thread+0x5c/0x64 Instruction dump: 7fe3fb78 48019689 80010014 7c630034 83e1000c 5463d97e 7c0803a6 38210010 4e800020 81250000 712a0001 41820008 <0fe00000> 9421ffe0 93e1001c 48000030 Implement unmap_kernel_page() which clears an existing pte.	N/A	More Details