SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 August 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-2024-7854	The Woo Inquiry plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 0.1 due to insufficient escaping on the user supplied parameter 'dbid' 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.	10.0	More Details
CVE-2024-4872	A vulnerability exists in the query validation of the MicroSCADA Pro/X SYS600 product. If exploited this could allow an authenticated attacker to inject code towards persistent data. Note that to successfully exploit this vulnerability an attacker must have a valid credential.	9.9	More Details
CVE-2024-3980	The MicroSCADA Pro/X SYS600 product allows an authenticated user input to control or influence paths or file names that are used in filesystem operations. If exploited the vulnerability allows the attacker to access or modify system files or other files that are critical to the application.	9.9	More Details
CVE-2024-6386	The WPML plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.6.12 via the Twig Server-Side Template Injection. This is due to missing input validation and sanitization on the render function. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.	9.9	More Details
CVE-2024-8161	SQL injection vulnerability in ATISolutions CIGES affecting versions lower than 2.15.5. This vulnerability allows a remote attacker to send a specially crafted SQL query to the /modules/ajaxServiciosCentro.php point in the idCentro parameter and retrieve all the information stored in the database.	9.8	More Details
CVE-2024-44563	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo.	9.8	More Details
CVE-2024-44565	Tenda AX1806 v1.0.0.1 contains a stack overflow via the serverName parameter in the function form_fast_setting_internet_set.	9.8	More Details
CVE-2024-44556	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo.	9.8	More Details
CVE-2024-44558	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo.	9.8	More Details
CVE-2024-44551	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45256	An arbitrary file write issue in the exfiltration endpoint in BYOB (Build Your Own Botnet) 2.0 allows attackers to overwrite SQLite databases and bypass authentication via an unauthenticated HTTP request with a crafted parameter. This occurs in file_add in api/files/routes.py.	9.8	More Details
CVE-2024-8073	Improper Input Validation vulnerability in Hillstone Networks Hillstone Networks Web Application Firewall on 5.5R6 allows Command Injection.This issue affects Hillstone Networks Web Application Firewall: from 5.5R6-2.6.7 through 5.5R6-2.8.13.	9.8	More Details
CVE-2024-8162	A vulnerability classified as critical has been found in TOTOLINK T10 AC1200 4.1.8cu.5207. Affected is an unknown function of the file /squashfs-root/web_cste/cgi-bin/product.ini of the component Telnet Service. The manipulation leads to hard-coded credentials. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2024-7988	A remote code execution vulnerability exists in the Rockwell Automation ThinManager® ThinServer™ that allows a threat actor to execute arbitrary code with System privileges. This vulnerability exists due to the lack of proper data input validation, which allows files to be overwritten.	9.8	More Details
CVE-2024-34087	An SEH-based buffer overflow in the BPQ32 HTTP Server in BPQ32 6.0.24.1 allows remote attackers with access to the Web Terminal to achieve remote code execution via an HTTP POST /TermInput request.	9.8	More Details
CVE-2024-41285	A stack overflow in FAST FW300R v1.3.13 Build 141023 Rel.61347n allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via a crafted file path.	9.8	More Details
CVE-2024-44549	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv.	9.8	More Details
CVE-2024-44550	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv.	9.8	More Details
CVE-2024-44553	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv.	9.8	More Details
CVE-2024-44552	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formGetIptv.	9.8	More Details
CVE-2024-45237	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a resource certificate containing a Key Usage extension composed of more than two bytes of data. Fort writes this string into a 2-byte buffer without properly sanitizing its length, leading to a buffer overflow.	9.8	More Details
CVE-2024-44555	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo.	9.8	More Details
CVE-2024-44557	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo.	9.8	More Details
CVE-2024-41444	SeaCMS v12.9 has a SQL injection vulnerability in the key parameter of /js/player/dmplayer/dmku/index.php?ac=so.	9.8	More Details
CVE-2024-42913	RuoYi CMS v4.7.9 was discovered to contain a SQL injection vulnerability via the job_id parameter at /sasfs1.	9.8	More Details
CVE-2024-45265	A SQL injection vulnerability in the poll component in SkySystem Arfa-CMS before 5.1.3124 allows remote attackers to execute arbitrary SQL commands via the psid parameter.	9.8	More Details
CVE-2024-8181	An Authentication Bypass vulnerability exists in Flowise version 1.8.2. This could allow a remote, unauthenticated attacker to access API endpoints as an administrator and allow them to access restricted functionality.	9.8	More Details
CVE-2024-7071	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 564 - SQL Injection: Hibernate vulnerability in Brain Information Technologies Inc. Brain Low-Code allows SQL Injection.This issue affects Brain Low-Code: before 2.1.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6633	The default credentials for the setup HSQL database (HSQLDB) for FileCatalyst Workflow are published in a vendor knowledgebase article. Misuse of these credentials could lead to a compromise of confidentiality, integrity, or availability of the software. The HSQLDB is only included to facilitate installation, has been deprecated, and is not intended for production use per vendor guides. However, users who have not configured FileCatalyst Workflow to use an alternative database per recommendations are vulnerable to attack from any source that can reach the HSQLDB.	9.8	More Details
CVE-2024-41622	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the tomography_ping_address parameter in /HNAP1/ interface.	9.8	More Details
CVE-2024-44341	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the lan(0)_dhcps_staticlist parameter. This vulnerability is exploited via a crafted POST request.	9.8	More Details
CVE-2024-44342	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the wl(0).(0)_ssid parameter. This vulnerability is exploited via a crafted POST request.	9.8	More Details
CVE-2024-36068	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code.	9.8	More Details
CVE-2024-45258	The req package before 3.43.4 for Go may send an unintended request when a malformed URL is provided, because cleanHost in http.go intentionally uses a "garbage in, garbage out" design.	9.8	More Details
CVE-2024-7720	HP Security Manager is potentially vulnerable to Remote Code Execution as a result of code vulnerability within the product's solution open-source libraries.	9.8	More Details
CVE-2024-5335	The Ultimate Store Kit Elementor Addons, Woocommerce Builder, EDD Builder, Elementor Store Builder, Product Grid, Product Table, Woocommerce Slider plugin is vulnerable to PHP Object Injection via deserialization of untrusted input via the _ultimate_store_kit_compare_products cookie in versions up to , and including, 1.6.4. This makes it possible for an unauthenticated attacker to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker or above to delete arbitrary files, retrieve sensitive data, or execute code.	9.8	More Details
CVE-2024-40766	An improper access control vulnerability has been identified in the SonicWall SonicOS management access, potentially leading to unauthorized resource access and in specific conditions, causing the firewall to crash. This issue affects SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.	9.8	More Details
CVE-2024-28000	Incorrect Privilege Assignment vulnerability in LiteSpeed Technologies LiteSpeed Cache litespeed-cache allows Privilege Escalation.This issue affects LiteSpeed Cache: from 1.9 through 6.3.0.1.	9.8	More Details
CVE-2024-40453	squirrellyjs squirrelly v9.0.0 and fixed in v.9.0.1 was discovered to contain a code injection vulnerability via the component options.varName.	9.8	More Details
CVE-2024-42777	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=signup" of Kashipara Music Management System v1.0, which allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2024-42781	A SQL injection vulnerability in "/music/ajax.php?action=login" of Kashipara Music Management System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the email parameter.	9.8	More Details
CVE-2024-42782	A SQL injection vulnerability in "/music/ajax.php?action=find_music" in Kashipara Music Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "search" parameter.	9.8	More Details
CVE-2024-42783	Kashipara Music Management System v1.0 is vulnerable to SQL Injection via /music/manage_playlist_items.php. An attacker can execute arbitrary SQL commands via the "pid" parameter.	9.8	More Details
CVE-2024-42784	A SQL injection vulnerability in "/music/controller.php?page=view_music" in Kashipara Music Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "id" parameter.	9.8	More Details
CVE-2024-45166	An issue was discovered in UCI IDOL 2 (aka uciIDOL or IDOL2) through 2.12. Due to improper input validation, improper deserialization, and improper restriction of operations within the bounds of a memory buffer, IDOL2 is vulnerable to Denial-of-Service (DoS) attacks and possibly remote code execution. There is an access violation and EIP overwrite after five logins.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45167	An issue was discovered in UCI IDOL 2 (aka uciIDOL or IDOL2) through 2.12. Due to improper input validation, improper deserialization, and improper restriction of operations within the bounds of a memory buffer, IDOL2 is vulnerable to Denial-of-Service (DoS) attacks and possibly remote code execution. A certain XmlMessage document causes 100% CPU consumption.	9.8	More Details
CVE-2024-45169	An issue was discovered in UCI IDOL 2 (aka uciIDOL or IDOL2) through 2.12. Due to improper input validation, improper deserialization, and improper restriction of operations within the bounds of a memory buffer, IDOL2 is vulnerable to Denial-of-Service (DoS) attacks and possibly remote code execution via the \xB0\x00\x3c byte sequence.	9.8	More Details
CVE-2024-36445	Swissphone DiCal-RED 4009 devices allow a remote attacker to gain a root shell via TELNET without authentication.	9.8	More Details
CVE-2024-7954	The porte_plume plugin used by SPIP before 4.30-alpha2, 4.2.13, and 4.1.16 is vulnerable to an arbitrary code execution vulnerability. A remote and unauthenticated attacker can execute arbitrary PHP as the SPIP user by sending a crafted HTTP request.	9.8	More Details
CVE-2024-42531	Ezviz Internet PT Camera CS-CV246 D15655150 allows an unauthenticated host to access its live video stream by crafting a set of RTSP packets with a specific set of URLs that can be used to redirect the camera feed. NOTE: the vendor's perspective is that the Anonymous120386 sample code can establish RTSP protocol communictaion, but cannot obtain video or audio data; thus, there is no risk.	9.8	More Details
CVE-2024-42765	A SQL injection vulnerability in "/login.php" of the Kashipara Bus Ticket Reservation System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the "email" or "password" Login page parameters.	9.8	More Details
CVE-2024-44381	D-Link DI_8004W 16.07.26A1 contains a command execution vulnerability in jhttpd msp_info_htm function.	9.8	More Details
CVE-2024-44382	D-Link DI_8004W 16.07.26A1 contains a command execution vulnerability in the jhttpd upgrade_filter_asp function.	9.8	More Details
CVE-2024-32501	A SQL Injection vulnerability exists in the updateServiceHost functionality in Centreon Web 24.04.x before 24.04.3, 23.10.x before 23.10.13, 23.04.x before 23.04.19, and 22.10.x before 22.10.23.	9.8	More Details
CVE-2024-7568	The Favicon Generator plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5. This is due to missing or incorrect nonce validation on the output_sub_admin_page_0 function. This makes it possible for unauthenticated attackers to delete arbitrary files on the server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The plugin author deleted the functionality of the plugin to patch this issue and close the plugin, we recommend seeking an alternative to this plugin.	9.6	More Details
CVE-2023-6452	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Forcepoint Web Security (Transaction Viewer) allows Stored XSS. The Forcepoint Web Security portal allows administrators to generate detailed reports on user requests made through the Web proxy. It has been determined that the "user agent" field in the Transaction Viewer is vulnerable to a persistent Cross-Site Scripting (XSS) vulnerability, which can be exploited by any user who can route traffic through the Forcepoint Web proxy. This vulnerability enables unauthorized attackers to execute JavaScript within the browser context of a Forcepoint administrator, thereby allowing them to perform actions on the administrator's behalf. Such a breach could lead to unauthorized access or modifications, posing a significant security risk. This issue affects Web Security: before 8.5.6.	9.6	More Details
CVE-2024-7971	Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2024-36439	Swissphone DiCal-RED 4009 devices allow a remote attacker to gain access to the administrative web interface via the device password's hash value, without knowing the actual device password.	9.4	More Details
CVE-2024-42764	Kashipara Bus Ticket Reservation System v1.0 is vulnerable to Cross Site Request Forgery (CSRF) via /deleteTicket.php.	9.4	More Details
CVE-2024-33852	A SQL Injection vulnerability exists in the Downtime component in Centreon Web 24.04.x before 24.04.3, 23.10.x before 23.10.13, 23.04.x before 23.04.19, and 22.10.x before 22.10.23.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33854	A SQL Injection vulnerability exists in the Graph Template component in Centreon Web 24.04.x before 24.04.3, 23.10.x before 23.10.13, 23.04.x before 23.04.19, and 22.10.x before 22.10.23.	9.1	More Details
CVE-2024-33853	A SQL Injection vulnerability exists in the Timeperiod component in Centreon Web 24.04.x before 24.04.3, 23.10.x before 23.10.13, 23.04.x before 23.04.19, and 22.10.x before 22.10.23.	9.1	More Details
CVE-2024-42773	An Incorrect Access Control vulnerability was found in /admin/edit_room_controller.php in Kashipara Hotel Management System v1.0, which allows an unauthenticated attacker to edit the valid hotel room entries in the administrator section.	9.1	More Details
CVE-2024-42775	An Incorrect Access Control vulnerability was found in /admin/add_room_controller.php in Kashipara Hotel Management System v1.0, which allows an unauthenticated attacker to add the valid hotel room entries in the administrator section via the direct URL access.	9.1	More Details
CVE-2024-45163	The Mirai botnet through 2024-08-19 mishandles simultaneous TCP connections to the CNC (command and control) server. Unauthenticated sessions remain open, causing resource consumption. For example, an attacker can send a recognized username (such as root), or can send arbitrary data.	9.1	More Details
CVE-2024-45168	An issue was discovered in UCI IDOL 2 (aka uciIDOL or IDOL2) through 2.12. Data is transferred over a raw socket without any authentication mechanism. Thus, communication endpoints are not verifiable.	9.1	More Details
CVE-2024-42914	A host header injection vulnerability exists in the forgot password functionality of ArrowCMS version 1.0.0. By sending a specially crafted host header in the forgot password request, it is possible to send password reset links to users which, once clicked, lead to an attacker-controlled server and thus leak the password reset token. This may allow an attacker to reset other users' passwords.	9.1	More Details
CVE-2024-28987	The SolarWinds Web Help Desk (WHD) software is affected by a hardcoded credential vulnerability, allowing remote unauthenticated user to access internal functionality and modify data.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-8225	A vulnerability, which was classified as critical, was found in Tenda G3 15.11.0.20. Affected is the function formSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument sysTimePolicy leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-7559	The File Manager Pro plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation and capability checks in the mk_file_folder_manager AJAX action in all versions up to, and including, 8.3.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-45264	A cross-site request forgery (CSRF) vulnerability in the admin panel in SkySystem Arfa-CMS before 5.1.3124 allows remote attackers to add a new administrator, leading to escalation of privileges.	8.8	More Details
CVE-2024-44340	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via keys smartqos_express_devices and smartqos_normal_devices in SetSmartQoSSettings.	8.8	More Details
CVE-2024-7258	The WooCommerce Google Feed Manager plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'wppfm_removeFeedFile' function in all versions up to, and including, 2.8.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.8	More Details
CVE-2024-42786	A SQL injection vulnerability in "/music/view_user.php" in Kashipara Music Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "id" parameter of View User Profile Page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42785	A SQL injection vulnerability in /music/index.php?page=view_playlist in Kashipara Music Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "id" parameter.	8.8	More Details
CVE-2024-42780	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_genre" in Kashipara Music Management System v1.0. This allows attackers to execute arbitrary code via uploading a crafted PHP file.	8.8	More Details
CVE-2024-42779	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_music" in Kashipara Music Management System v1.0. This allows attackers to execute arbitrary code via uploading a crafted PHP file.	8.8	More Details
CVE-2024-42778	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_playlist" in Kashipara Music Management System v1.0. This allows attackers to execute arbitrary code via uploading a crafted PHP file.	8.8	More Details
CVE-2024-5725	Centreon initCurveList SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the initCurveList function. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of the apache user. Was ZDI-CAN-22683.	8.8	More Details
CVE-2024-5723	Centreon updateServiceHost SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the updateServiceHost function. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of the apache user. Was ZDI-CAN-23294.	8.8	More Details
CVE-2024-7795	Autel MaxiCharger AC Elite Business C50 AppAuthenExchangeRandomNum Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the AppAuthenExchangeRandomNum BLE command. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23384.	8.8	More Details
CVE-2024-7966	Out of bounds memory access in Skia in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had compromised the renderer process to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-42599	SeaCMS 13.0 has a remote code execution vulnerability. The reason for this vulnerability is that although admin_files.php imposes restrictions on edited files, attackers can still bypass these restrictions and write code, allowing authenticated attackers to exploit the vulnerability to execute arbitrary commands and gain system privileges.	8.8	More Details
CVE-2024-7725	Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23928.	8.8	More Details
CVE-2024-7724	Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23900.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7723	Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23736.	8.8	More Details
CVE-2024-6814	NETGEAR ProSAFE Network Management System getFilterString SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getFilterString method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-23399.	8.8	More Details
CVE-2024-6813	NETGEAR ProSAFE Network Management System getSortString SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getSortString method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-23207.	8.8	More Details
CVE-2024-8079	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been rated as critical. This issue affects the function exportOvpn. The manipulation leads to buffer overflow. The attack may be initiated remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-8078	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been declared as critical. This vulnerability affects the function setTracerouteCfg. The manipulation leads to buffer overflow. The attack can be initiated remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-42791	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via /music/ajax.php?action=delete_genre.	8.8	More Details
CVE-2024-8076	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228 and classified as critical. Affected by this issue is the function setDiagnosisCfg. The manipulation leads to buffer overflow. The attack may be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-7965	Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-7964	Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-7967	Heap buffer overflow in Fonts in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-36442	cgi-bin/fdmcgiwebv2.cgi on Swissphone DiCal-RED 4009 devices allows an authenticated attacker to gain access to arbitrary files on the device's file system.	8.8	More Details
CVE-2024-8224	A vulnerability, which was classified as critical, has been found in Tenda G3 15.11.0.20. This issue affects the function formSetDebugCfg of the file /goform/setDebugCfg. The manipulation of the argument enable/level/module leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-39576	Dell Power Manager (DPM), versions 3.15.0 and prior, contains an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Elevation of privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5466	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option.	8.8	More Details
CVE-2024-42756	An issue in Netgear DGN1000WW v.1.1.00.45 allows a remote attacker to execute arbitrary code via the Diagnostics page	8.8	More Details
CVE-2024-39841	A SQL Injection vulnerability exists in the service configuration functionality in Centreon Web 24.04.x before 24.04.3, 23.10.x before 23.10.13, 23.04.x before 23.04.19, and 22.10.x before 22.10.23.	8.8	More Details
CVE-2024-44390	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the function formWrlsafeset.	8.8	More Details
CVE-2024-43033	JPress through 5.1.1 on Windows has an arbitrary file upload vulnerability that could cause arbitrary code execution via ::$DATA to AttachmentController, such as a .jsp::$DATA file to io.jpress.web.commons.controller.AttachmentController#upload. NOTE: this is unrelated to the attack vector for CVE-2024-32358.	8.8	More Details
CVE-2024-7972	Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-7974	Insufficient data validation in V8 API in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-7968	Use after free in Autofill in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-7969	Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-7656	The Image Hotspot by DevVN plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.2.5 via deserialization of untrusted input in the 'devvn_ihotspot_shortcode_func' function. This makes it possible for authenticated attackers, with Author-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-7973	Heap buffer overflow in PDFium in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-45201	An issue was discovered in llama_index before 0.10.38. download/integration.py includes an exec call for import {cls_name}.	8.8	More Details
CVE-2020-11846	A vulnerability found in OpenText Privileged Access Manager that issues a token. on successful issuance of the token, a cookie gets set that allows unrestricted access to all the application resources. This issue affects Privileged Access Manager before 3.7.0.1.	8.7	More Details
CVE-2024-43798	Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. The Chisel server doesn't ever read the documented `AUTH` environment variable used to set credentials, which allows any unauthenticated user to connect, even if credentials were set. Anyone running the Chisel server that is using the `AUTH` environment variable to specify credentials to authenticate against is affected by this vulnerability. Chisel is often used to provide an entrypoint to a private network, which means services that are gated by Chisel may be affected. Additionally, Chisel is often used for exposing services to the internet. An attacker could MITM requests by connecting to a Chisel server and requesting to forward traffic from a remote port. This issue has been addressed in release version 1.10.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20375	A vulnerability in the SIP call processing function of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a crafted SIP message to an affected Cisco Unified CM or Cisco Unified CM SME device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition that interrupts the communications of reliant voice and video devices.	8.6	More Details
CVE-2024-36514	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in file summary option.	8.3	More Details
CVE-2024-38869	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25.	8.3	More Details
CVE-2024-5586	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in extranet lockouts report option.	8.3	More Details
CVE-2024-42340	CyberArk - CWE-602: Client-Side Enforcement of Server-Side Security	8.3	More Details
CVE-2024-5556	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in reports module.	8.3	More Details
CVE-2024-5490	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in aggregate reports option.	8.3	More Details
CVE-2024-36517	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in alerts module.	8.3	More Details
CVE-2024-36516	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in dashboard. Note: This vulnerability is different from another vulnerability (CVE-2024-36515), both of which have affected ADAudit Plus' dashboard.	8.3	More Details
CVE-2024-36515	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in dashboard. Note: This vulnerability is different from another vulnerability (CVE-2024-36516), both of which have affected ADAudit Plus' dashboard.	8.3	More Details
CVE-2024-5467	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in account lockout report.	8.3	More Details
CVE-2024-7940	The product exposes a service that is intended for local only to all network interfaces without any authentication.	8.3	More Details
CVE-2024-3982	An attacker with local access to machine where MicroSCADA X SYS600 is installed, could enable the session logging supporting the product and try to exploit a session hijacking of an already established session. By default, the session logging level is not enabled and only users with administrator rights can enable it.	8.2	More Details
CVE-2024-43444	Passwords of agents and customers are displayed in plain text in the OTRS admin log module if certain configurations regarding the authentication sources match and debugging for the authentication backend has been enabled. This issue affects: * OTRS from 7.0.X through 7.0.50 * OTRS 8.0.X * OTRS 2023.X * OTRS from 2024.X through 2024.5.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	8.2	More Details
CVE-2024-37311	Collabora Online is a collaborative online office suite based on LibreOffice. In affected versions of Collabora Online, https connections from coolwsd to other hosts may incompletely verify the remote host's certificate's against the full chain of trust. This vulnerability is fixed in Collabora Online 24.04.4.3, 23.05.14.1, and 22.05.23.1.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11847	SSH authenticated user when access the PAM server can execute an OS command to gain the full system access using bash. This issue affects Privileged Access Manager before 3.7.0.1.	8.2	More Details
CVE-2024-45321	The App::cpanminus package through 1.7047 for Perl downloads code via insecure HTTP, enabling code execution for network attackers.	8.1	More Details
CVE-2024-7601	Logsign Unified SecOps Platform Directory data_export_delete_all Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of root. Was ZDI-CAN-25026.	8.1	More Details
CVE-2024-8007	A flaw was found in the openstack-tripleo-common component of the Red Hat OpenStack Platform (RHOSP) director. This vulnerability allows an attacker to deploy potentially compromised container images via disabling TLS certificate verification for registry mirrors, which could enable a man-in-the-middle (MITM) attack.	8.1	More Details
CVE-2024-5762	Zen Cart findPluginAdminPage Local File Inclusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Zen Cart. Authentication is not required to exploit this vulnerability. The specific flaw exists within the findPluginAdminPage function. The issue results from the lack of proper validation of user-supplied data prior to passing it to a PHP include function. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the service account. Was ZDI-CAN-21408.	8.1	More Details
CVE-2024-7600	Logsign Unified SecOps Platform Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of root. Was ZDI-CAN-25025.	8.1	More Details
CVE-2024-42040	Buffer Overflow vulnerability in the net/bootp.c in DENEX U-Boot from its initial commit in 2002 (3861aa5) up to today on any platform allows an attacker on the local network to leak memory from four up to 32 bytes of memory stored behind the packet to the network depending on the later use of DHCP-provided parameters via crafted DHCP responses.	8.1	More Details
CVE-2024-7603	Logsign Unified SecOps Platform Directory Traversal Arbitrary Directory Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary directories on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete directories in the context of root. Was ZDI-CAN-25028.	8.1	More Details
CVE-2024-36444	cgi-bin/fdmcgiwebv2.cgi on Swissphone DiCal-RED 4009 devices allows an unauthenticated attacker to gain access to device logs.	8.1	More Details
CVE-2024-39344	An issue was discovered in the Docusign API package 8.142.14 for Salesforce. The Apttus_DocuApi__DocusignAuthentication__mdt object is installed via the marketplace from this package and stores some configuration information in a manner that could be compromised. With the default settings when installed for all users, the object can be accessible and (via its fields) could disclose some keys. These disclosed components can be combined to create a valid session via the Docusign API. This will generally lead to a complete compromise of the Docusign account because the session is for an administrator service account and may have permission to re-authenticate as specific users with the same authorization flow.	8.1	More Details
CVE-2024-42845	An eval Injection vulnerability in the component invesalius/reader/dicom.py of InVesalius 3.1.99991 through 3.1.99998 allows attackers to execute arbitrary code via loading a crafted DICOM file.	8.0	More Details
CVE-2022-39997	A weak password requirement issue was discovered in Teldats Router RS123, RS123w allows a remote attacker to escalate privileges	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6508	An insufficient entropy vulnerability was found in the Openshift Console. In the authorization code type and implicit grant type, the OAuth2 protocol is vulnerable to a Cross-Site Request Forgery (CSRF) attack if the state parameter is used inefficiently. This flaw allows logging into the victim's current application account using a third-party account without any restrictions.	8.0	More Details
CVE-2024-7448	Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Magnet Forensics AXIOM. User interaction is required to exploit this vulnerability in that the target must acquire data from a malicious mobile device. The specific flaw exists within the Android device image acquisition functionality. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-23964.	8.0	More Details
CVE-2024-43027	DrayTek Vigor 3900 before v1.5.1.5_Beta, DrayTek Vigor 2960 before v1.5.1.5_Beta and DrayTek Vigor 300B before v1.5.1.5_Beta were discovered to contain a command injection vulnerability via the action parameter at cgi-bin/mainfunction.cgi.	8.0	More Details
CVE-2024-42915	A host header injection vulnerability in Staff Appraisal System v1.0 allows attackers to obtain the password reset token via user interaction with a crafted password reset link. This will allow attackers to arbitrarily reset other users' passwords and compromise their accounts.	8.0	More Details
CVE-2022-48943	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: make apf token non-zero to fix bug In current async pagefault logic, when a page is ready, KVM relies on kvm_arch_can_dequeue_async_page_present() to determine whether to deliver a READY event to the Guest. This function test token value of struct kvm_vcpu_pv_apf_data, which must be reset to zero by Guest kernel when a READY event is finished by Guest. If value is zero meaning that a READY event is done, so the KVM can deliver another. But the kvm_arch_setup_async_pf() may produce a valid token with zero value, which is confused with previous mention and may lead the loss of this READY event. This bug may cause task blocked forever in Guest: INFO: task stress:7532 blocked for more than 1254 seconds. Not tainted 5.10.0 #16 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:stress state:D stack: 0 pid: 7532 ppid: 1409 flags:0x00000080 Call Trace: __schedule+0x1e7/0x650 schedule+0x46/0xb0 kvm_async_pf_task_wait_schedule+0xad/0xe0 ? exit_to_user_mode_prepare+0x60/0x70 __kvm_handle_async_pf+0x4f/0xb0 ? asm_exc_page_fault+0x8/0x30 exc_page_fault+0x6f/0x110 ? asm_exc_page_fault+0x8/0x30 asm_exc_page_fault+0x1e/0x30 RIP: 0033:0x402d00 RSP: 002b:00007ffd31912500 EFLAGS: 00010206 RAX: 0000000000071000 RBX: ffffffffffffffff RCX: 00000000021a32b0 RDX: 000000000007d011 RSI: 000000000007d000 RDI: 00000000021262b0 RBP: 00000000021262b0 R08: 0000000000000003 R09: 0000000000000086 R10: 00000000000000eb R11: 00007fefbdf2baa0 R12: 0000000000000000 R13: 0000000000000002 R14: 000000000007d000 R15: 0000000000001000	7.8	More Details
CVE-2022-48926	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4 [361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c	7.8	More Details
CVE-2022-48867	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Prevent use after free on completion memory On driver unload any pending descriptors are flushed at the time the interrupt is freed: idxd_dmaengine_drv_remove() -> drv_disable_wq() -> idxd_wq_free_irq() -> idxd_flush_pending_descs(). If there are any descriptors present that need to be flushed this flow triggers a "not present" page fault as below: BUG: unable to handle page fault for address: ff391c97c70c9040 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page The address that triggers the fault is the address of the descriptor that was freed moments earlier via: drv_disable_wq()->idxd_wq_free_resources() Fix the use after free by freeing the descriptors after any possible usage. This is done after idxd_wq_reset() to ensure that the memory remains accessible during possible completion writes by the device.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37008	A maliciously crafted DWG file, when parsed in Revit, can force a stack-based buffer overflow. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-42851	Buffer Overflow vulnerability in open source exiftags v.1.01 allows a local attacker to execute arbitrary code via the paresetag function.	7.8	More Details
CVE-2024-33657	This SMM vulnerability affects certain modules, allowing privileged attackers to execute arbitrary code, manipulate stack memory, and leak information from SMRAM to kernel space, potentially leading to denial-of-service attacks.	7.8	More Details
CVE-2024-7604	Logsign Unified SecOps Platform Incorrect Authorization Authentication Bypass Vulnerability. This vulnerability allows local attackers to bypass authentication on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of the user's license expiration date. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-25029.	7.8	More Details
CVE-2022-48874	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix use-after-free and race in fastrpc_map_find Currently, there is a race window between the point when the mutex is unlocked in fastrpc_map_lookup and the reference count increasing (fastrpc_map_get) in fastrpc_map_find, which can also lead to use-after-free. So lets merge fastrpc_map_find into fastrpc_map_lookup which allows us to both protect the maps list by also taking the &fl->lock spinlock and the reference count, since the spinlock will be released only after. Add take_ref argument to make this suitable for all callers.	7.8	More Details
CVE-2022-48873	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Don't remove map on creater_process and device_release Do not remove the map from the list on error path in fastrpc_init_create_process, instead call fastrpc_map_put, to avoid use-after-free. Do not remove it on fastrpc_device_release either, call fastrpc_map_put instead. The fastrpc_free_map is the only proper place to remove the map. This is called only after the reference count is 0.	7.8	More Details
CVE-2024-5929	VIPRE Advanced Security PMAgent Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Patch Management Agent. The issue results from loading a file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-22316.	7.8	More Details
CVE-2024-6812	IrfanView WSQ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WSQ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23273.	7.8	More Details
CVE-2024-7013	Stack-based buffer overflow in Control FPWIN Pro version 7.7.2.0 and all previous versions may allow attackers to execute arbitrary code via a specially crafted project file.	7.8	More Details
CVE-2024-6811	IrfanView WSQ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WSQ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24192.	7.8	More Details
CVE-2024-6141	Windscribe Directory Traversal Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Windscribe. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Windscribe Service. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23441.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38210	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-5928	VIPRE Advanced Security PMAgent Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Patch Management Agent. By creating a symbolic link, an attacker can abuse the agent to delete a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-22315.	7.8	More Details
CVE-2024-5930	VIPRE Advanced Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Anti Malware Service. The issue results from incorrect permissions on a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-22345.	7.8	More Details
CVE-2024-38209	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-7125	Authentication Bypass vulnerability in Hitachi Ops Center Common Services.This issue affects Hitachi Ops Center Common Services: from 10.9.3-00 before 11.0.2-01.	7.8	More Details
CVE-2024-33656	The DXE module SmmComputrace contains a vulnerability that allows local attackers to leak stack or global memory. This could lead to privilege escalation, arbitrary code execution, and bypassing OS security mechanisms	7.8	More Details
CVE-2024-41879	Acrobat Reader versions 127.0.2651.105 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-48927	In the Linux kernel, the following vulnerability has been resolved: iio: adc: tsc2046: fix memory corruption by preventing array overflow On one side we have indio_dev->num_channels includes all physical channels + timestamp channel. On other side we have an array allocated only for physical channels. So, fix memory corruption by ARRAY_SIZE() instead of num_channels variable. Note the first case is a cleanup rather than a fix as the software timestamp channel bit in active_scanmask is never set by the IIO core.	7.8	More Details
CVE-2022-48925	In the Linux kernel, the following vulnerability has been resolved: RDMA/cma: Do not change route.addr.src_addr outside state checks If the state is not idle then resolve_prepare_src() should immediately fail and no change to global state should happen. However, it unconditionally overwrites the src_addr trying to build a temporary any address. For instance if the state is already RDMA_CM_LISTEN then this will corrupt the src_addr and would cause the test in cma_cancel_operation(): if (cma_any_addr(cma_src_addr(id_priv)) && !id_priv->cma_dev) Which would manifest as this trace from syzkaller: BUG: KASAN: use-after-free in __list_add_valid+0x93/0xa0 lib/list_debug.c:26 Read of size 8 at addr ffff8881546491e0 by task syz-executor.1/32204 CPU: 1 PID: 32204 Comm: syz-executor.1 Not tainted 5.12.0-rc8-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:79 [inline] dump_stack+0x141/0x1d7 lib/dump_stack.c:120 print_address_description.constprop.0.cold+0x5b/0x2f8 mm/kasan/report.c:232 __kasan_report mm/kasan/report.c:399 [inline] kasan_report.cold+0x7c/0xd8 mm/kasan/report.c:416 __list_add_valid+0x93/0xa0 lib/list_debug.c:26 __list_add include/linux/list.h:67 [inline] list_add_tail include/linux/list.h:100 [inline] cma_listen_on_all drivers/infiniband/core/cma.c:2557 [inline] rdma_listen+0x787/0xe00 drivers/infiniband/core/cma.c:3751 ucma_listen+0x16a/0x210 drivers/infiniband/core/ucma.c:1102 ucma_write+0x259/0x350 drivers/infiniband/core/ucma.c:1732 vfs_write+0x28e/0xa30 fs/read_write.c:603 ksys_write+0x1ee/0x250 fs/read_write.c:658 do_syscall_64+0x2d/0x70 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae This is indicating that an rdma_id_private was destroyed without doing cma_cancel_listens(). Instead of trying to re-use the src_addr memory to indirectly create an any address derived from the dst build one explicitly on the stack and bind to that as any other normal flow would do. rdma_bind_addr() will copy it over the src_addr once it knows the state is valid. This is similar to commit bc0bdc5afaa7 ("RDMA/cma: Do not change route.addr.src_addr.ss_family")	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48919	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae	7.8	More Details
CVE-2022-48892	In the Linux kernel, the following vulnerability has been resolved: sched/core: Fix use-after-free bug in dup_user_cpus_ptr() Since commit 07ec77a1d4e8 ("sched: Allow task CPU affinity to be restricted on asymmetric systems"), the setting and clearing of user_cpus_ptr are done under pi_lock for arm64 architecture. However, dup_user_cpus_ptr() accesses user_cpus_ptr without any lock protection. Since sched_setaffinity() can be invoked from another process, the process being modified may be undergoing fork() at the same time. When racing with the clearing of user_cpus_ptr in __set_cpus_allowed_ptr_locked(), it can lead to user-after-free and possibly double-free in arm64 kernel. Commit 8f9ea86fdf99 ("sched: Always preserve the user requested cpumask") fixes this problem as user_cpus_ptr, once set, will never be cleared in a task's lifetime. However, this bug was re-introduced in commit 851a723e45d1 ("sched: Always clear user_cpus_ptr in do_set_cpus_allowed()") which allows the clearing of user_cpus_ptr in do_set_cpus_allowed(). This time, it will affect all arches. Fix this bug by always clearing the user_cpus_ptr of the newly cloned/forked task before the copying process starts and check the user_cpus_ptr state of the source task under pi_lock. Note to stable, this patch won't be applicable to stable releases. Just copy the new dup_user_cpus_ptr() function over.	7.8	More Details
CVE-2024-43791	RequestStore provides per-request global storage for Rack. The files published as part of request_store 1.3.2 have 0666 permissions, meaning that they are world-writable, which allows local users to execute arbitrary code. This version was published in 2017, and most production environments do not allow access for local users, so the chances of this being exploited are very low, given that the vast majority of users will have upgraded, and those that have not, if any, are not likely to be exposed.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48913	In the Linux kernel, the following vulnerability has been resolved: blktrace: fix use after free for struct blk_trace When tracing the whole disk, 'dropped' and 'msg' will be created under 'q->debugfs_dir' and 'bt->dir' is NULL, thus blk_trace_free() won't remove those files. What's worse, the following UAF can be triggered because of accessing stale 'dropped' and 'msg': == BUG: KASAN: use-after-free in blk_dropped_read+0x89/0x100 Read of size 4 at addr ffff88816912f3d8 by task blktrace/1188 CPU: 27 PID: 1188 Comm: blktrace Not tainted 5.17.0-rc4-next-20220217+ #469 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ?-20190727_073836-4 Call Trace: <TASK> dump_stack_lvl+0x34/0x44 print_address_description.constprop.0.cold+0xab/0x381 ? blk_dropped_read+0x89/0x100 ? blk_dropped_read+0x89/0x100 kasan_report.cold+0x83/0xdf ? blk_dropped_read+0x89/0x100 kasan_check_range+0x140/0x1b0 blk_dropped_read+0x89/0x100 ? blk_create_buf_file_callback+0x20/0x20 ? kmem_cache_free+0xa1/0x500 ? do_sys_openat2+0x258/0x460 full_proxy_read+0x8f/0xc0 vfs_read+0xc6/0x260 ksys_read+0xb9/0x150 ? vfs_write+0x3d0/0x3d0 ? fpregs_assert_state_consistent+0x55/0x60 ? exit_to_user_mode_prepare+0x39/0x1e0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fbc080d92fd Code: ce 20 00 00 75 10 b8 00 00 00 00 0f 05 48 3d 01 f0 ff ff 73 31 c3 48 83 1 RSP: 002b:00007fbb95ff9cb0 EFLAGS: 00000293 ORIG_RAX: 0000000000000000 RAX: ffffffffffffffda RBX: 00007fbb95ff9dc0 RCX: 00007fbc080d92fd RDX: 0000000000000100 RSI: 00007fbb95ff9cc0 RDI: 0000000000000045 RBP: 0000000000000045 R08: 0000000000406299 R09: 00000000ffffffffd R10: 0000000000153afa0 R11: 0000000000000293 R12: 00007fbb780008c0 R13: 00007fbb78000938 R14: 0000000000608b30 R15: 00007fbb780029c8 </TASK> Allocated by task 1050: kasan_save_stack+0x1e/0x40 __kasan_kmalloc+0x81/0xa0 do_blk_trace_setup+0xcb/0x410 __blk_trace_setup+0xac/0x130 blk_trace_ioctl+0xe9/0x1c0 blkdev_ioctl+0xf1/0x390 __x64_sys_ioctl+0xa5/0xe0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae Freed by task 1050: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 kasan_set_free_info+0x20/0x30 __kasan_slab_free+0x103/0x180 kfree+0x9a/0x4c0 __blk_trace_remove+0x53/0x70 blk_trace_ioctl+0x199/0x1c0 blkdev_common_ioctl+0x5e9/0xb30 blkdev_ioctl+0x1a5/0x390 __x64_sys_ioctl+0xa5/0xe0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88816912f380 which belongs to the cache kmalloc-96 of size 96 The buggy address is located 88 bytes inside of 96-byte region [ffff88816912f380, ffff88816912f3e0) The buggy address belongs to the page: page:000000009a1b4e7c refcount:1 mapcount:0 mapping:0000000000000000 index:0x0f flags: 0x17ffffc0000200(slablnode=0lzone=2llastcpupid=0x1fffff) raw: 0017ffffc0000200 ffffea00044f1100 dead000000000002 ffff88810004c780 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff88816912f280: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f300: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc >ffff88816912f380: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ^ ffff88816912f400: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f480: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ==	7.8	More Details
CVE-2022-48878	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_qca: Fix driver shutdown on closed serdev The driver shutdown callback (which sends EDL_SOC_RESET to the device over serdev) should not be invoked when HCI device is not open (e.g. if hci_dev_open_sync() failed), because the serdev and its TTY are not open either. Also skip this step if device is powered off (qca_power_shutdown()). The shutdown callback causes use-after-free during system reboot with Qualcomm Atheros Bluetooth: Unable to handle kernel paging request at virtual address 0072662f67726fd7 ... CPU: 6 PID: 1 Comm: systemd-shutdow Tainted: G W 6.1.0-rt5-00325-g8a5f56bcfcca #8 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: tty_driver_flush_buffer+0x4/0x30 serdev_device_write_flush+0x24/0x34 qca_serdev_shutdown+0x80/0x130 [hci_uart] device_shutdown+0x15c/0x260 kernel_restart+0x48/0xac KASAN report: BUG: KASAN: use-after-free in tty_driver_flush_buffer+0x1c/0x50 Read of size 8 at addr ffff16270c2e0018 by task systemd-shutdow/1 CPU: 7 PID: 1 Comm: systemd-shutdow Not tainted 6.1.0-next-20221220-00014-gb85aaf97fb01-dirty #28 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: dump_backtrace.part.0+0xdc/0xf0 show_stack+0x18/0x30 dump_stack_lvl+0x68/0x84 print_report+0x188/0x488 kasan_report+0xa4/0xf0 __asan_load8+0x80/0xac tty_driver_flush_buffer+0x1c/0x50 ttyport_write_flush+0x34/0x44 serdev_device_write_flush+0x48/0x60 qca_serdev_shutdown+0x124/0x274 device_shutdown+0x1e8/0x350 kernel_restart+0x48/0xb0 __do_sys_reboot+0x244/0x2d0 __arm64_sys_reboot+0x54/0x70 invoke_syscall+0x60/0x190 el0_svc_common.constprop.0+0x7c/0x160 do_el0_svc+0x44/0xf0 el0_svc+0x2c/0x6c el0t_64_sync_handler+0xbc/0x140 el0t_64_sync+0x190/0x194	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48912	In the Linux kernel, the following vulnerability has been resolved: netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430 CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #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+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline] find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993 prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated---	7.8	More Details
CVE-2024-44942	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on F2FS_INLINE_DATA flag in inode during GC syzbot reports a f2fs bug as below: ------------[cut here]------------ kernel BUG at fs/f2fs/inline.c:258! CPU: 1 PID: 34 Comm: kworker/u8:2 Not tainted 6.9.0-rc6-syzkaller-00012-g9e4bc4bcae01 #0 RIP: 0010:f2fs_write_inline_data+0x781/0x790 fs/f2fs/inline.c:258 Call Trace: f2fs_write_single_data_page+0xb65/0x1d60 fs/f2fs/data.c:2834 f2fs_write_cache_pages fs/f2fs/data.c:3133 [inline] __f2fs_write_data_pages fs/f2fs/data.c:3288 [inline] f2fs_write_data_pages+0x1efe/0x3a90 fs/f2fs/data.c:3315 do_writepages+0x35b/0x870 mm/page-writeback.c:2612 __writeback_single_inode+0x165/0x10b0 fs/fs-writeback.c:1650 writeback_sb_inodes+0x905/0x1260 fs/fs-writeback.c:1941 wb_writeback+0x457/0xce0 fs/fs-writeback.c:2117 wb_do_writeback fs/fs-writeback.c:2264 [inline] wb_workfn+0x410/0x1090 fs/fs-writeback.c:2304 process_one_work kernel/workqueue.c:3254 [inline] process_scheduled_works+0xa12/0x17c0 kernel/workqueue.c:3335 worker_thread+0x86d/0xd70 kernel/workqueue.c:3416 kthread+0x2f2/0x390 kernel/kthread.c:388 ret_from_fork+0x4d/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244 The root cause is: inline_data inode can be fuzzed, so that there may be valid blkaddr in its direct node, once f2fs triggers background GC to migrate the block, it will hit f2fs_bug_on() during dirty page writeback. Let's add sanity check on F2FS_INLINE_DATA flag in inode during GC, so that, it can forbid migrating inline_data inode's data block for fixing.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44941	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to cover read extent cache access with lock syzbot reports a f2fs bug as below: BUG: KASAN: slab-use-after-free in sanity_check_extent_cache+0x370/0x410 fs/f2fs/extent_cache.c:46 Read of size 4 at addr ffff8880739ab220 by task syz-executor200/5097 CPU: 0 PID: 5097 Comm: syz-executor200 Not tainted 6.9.0-rc6-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 sanity_check_extent_cache+0x370/0x410 fs/f2fs/extent_cache.c:46 do_read_inode fs/f2fs/inode.c:509 [inline] f2fs_iget+0x33e1/0x46e0 fs/f2fs/inode.c:560 f2fs_nfs_get_inode+0x74/0x100 fs/f2fs/super.c:3237 generic_fh_to_dentry+0x9f/0xf0 fs/libfs.c:1413 exportfs_decode_fh_raw+0x152/0x5f0 fs/exportfs/expfs.c:444 exportfs_decode_fh+0x3c/0x80 fs/exportfs/expfs.c:584 do_handle_to_path fs/fhandle.c:155 [inline] handle_to_path fs/fhandle.c:210 [inline] do_handle_open+0x495/0x650 fs/fhandle.c:226 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 We missed to cover sanity_check_extent_cache() w/ extent cache lock, so, below race case may happen, result in use after free issue. - f2fs_iget - do_read_inode - f2fs_init_read_extent_tree : add largest extent entry in to cache - shrink - f2fs_shrink_read_extent_tree - __shrink_extent_tree - __detach_extent_node : drop largest extent entry - sanity_check_extent_cache : access et->largest w/o lock let's refactor sanity_check_extent_cache() to avoid extent cache access and call it before f2fs_init_read_extent_tree() to fix this issue.	7.8	More Details
CVE-2024-44940	In the Linux kernel, the following vulnerability has been resolved: fou: remove warn in gue_gro_receive on unsupported protocol Drop the WARN_ON_ONCE inn gue_gro_receive if the encapsulated type is not known or does not have a GRO handler. Such a packet is easily constructed. Syzbot generates them and sets off this warning. Remove the warning as it is expected and not actionable. The warning was previously reduced from WARN_ON to WARN_ON_ONCE in commit 270136613bf7 ("fou: Do WARN_ON_ONCE in gue_gro_receive for bad proto callbacks").	7.8	More Details
CVE-2024-41173	The IPC-Diagnostics package included in TwinCAT/BSD is vulnerable to a local authentication bypass by a low privileged attacker.	7.8	More Details
CVE-2024-7980	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43900	In the Linux kernel, the following vulnerability has been resolved: media: xc2028: avoid use-after-free in load_firmware_cb() syzkaller reported use-after-free in load_firmware_cb() [1]. The reason is because the module allocated a struct tuner in tuner_probe(), and then the module initialization failed, the struct tuner was released. A worker which created during module initialization accesses this struct tuner later, it caused use-after-free. The process is as follows: task-6504 worker_thread tuner_probe <= alloc dvb_frontend [2] ... request_firmware_nowait <= create a worker ... tuner_remove <= free dvb_frontend ... request_firmware_work_func <= the firmware is ready load_firmware_cb <= but now the dvb_frontend has been freed To fix the issue, check the dvd_frontend in load_firmware_cb(), if it is null, report a warning and just return. [1]: == BUG: KASAN: use-after-free in load_firmware_cb+0x1310/0x17a0 Read of size 8 at addr ffff8000d7ca2308 by task kworker/2:3/6504 Call trace: load_firmware_cb+0x1310/0x17a0 request_firmware_work_func+0x128/0x220 process_one_work+0x770/0x1824 worker_thread+0x488/0xea0 kthread+0x300/0x430 ret_from_fork+0x10/0x20 Allocated by task 6504: kzalloc tuner_probe+0xb0/0x1430 i2c_device_probe+0x92c/0xaf0 really_probe+0x678/0xcd0 driver_probe_device+0x280/0x370 __device_attach_driver+0x220/0x330 bus_for_each_drv+0x134/0x1c0 __device_attach+0x1f4/0x410 device_initial_probe+0x20/0x30 bus_probe_device+0x184/0x200 device_add+0x924/0x12c0 device_register+0x24/0x30 i2c_new_device+0x4e0/0xc44 v4l2_i2c_new_subdev_board+0xbc/0x290 v4l2_i2c_new_subdev+0xc8/0x104 em28xx_v4l2_init+0x1dd0/0x3770 Freed by task 6504: kfree+0x238/0x4e4 tuner_remove+0x144/0x1c0 i2c_device_remove+0xc8/0x290 __device_release_driver+0x314/0x5fc device_release_driver+0x30/0x44 bus_remove_device+0x244/0x490 device_del+0x350/0x900 device_unregister+0x28/0xd0 i2c_unregister_device+0x174/0x1d0 v4l2_device_unregister+0x224/0x380 em28xx_v4l2_init+0x1d90/0x3770 The buggy address belongs to the object at ffff8000d7ca2000 which belongs to the cache kmalloc-2k of size 2048 The buggy address is located 776 bytes inside of 2048-byte region [ffff8000d7ca2000, ffff8000d7ca2800) The buggy address belongs to the page: page:ffff7fe00035f280 count:1 mapcount:0 mapping:ffff8000c001f000 index:0x0 flags: 0x7ff800000000100(slab) raw: 07ff800000000100 ffff7fe00049d880 0000000300000003 ffff8000c001f000 raw: 0000000000000000 0000000080100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8000d7ca2200: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8000d7ca2300: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8000d7ca2380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == [2] Actually, it is allocated for struct tuner, and dvb_frontend is inside.	7.8	More Details
CVE-2024-7979	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium)	7.8	More Details
CVE-2023-52906	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_mpls: Fix warning during failed attribute validation The 'TCA_MPLS_LABEL' attribute is of 'NLA_U32' type, but has a validation type of 'NLA_VALIDATE_FUNCTION'. This is an invalid combination according to the comment above 'struct nla_policy': " Meaning of `validate' field, use via NLA_POLICY_VALIDATE_FN: NLA_BINARY Validation function called for the attribute. All other Unused - but note that it's a union " This can trigger the warning [1] in nla_get_range_unsigned() when validation of the attribute fails. Despite being of 'NLA_U32' type, the associated 'min'/'max' fields in the policy are negative as they are aliased by the 'validate' field. Fix by changing the attribute type to 'NLA_BINARY' which is consistent with the above comment and all other users of NLA_POLICY_VALIDATE_FN(). As a result, move the length validation to the validation function. No regressions in MPLS tests: # ./tdc.py -f tc-tests/actions/mpls.json [...] # echo $? 0 [1] WARNING: CPU: 0 PID: 17743 at lib/nlattr.c:118 nla_get_range_unsigned+0x1d8/0x1e0 lib/nlattr.c:117 Modules linked in: CPU: 0 PID: 17743 Comm: syz-executor.0 Not tainted 6.1.0-rc8 #3 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.13.0-48-gd9c812dda519-prebuilt.qemu.org 04/01/2014 RIP: 0010:nla_get_range_unsigned+0x1d8/0x1e0 lib/nlattr.c:117 [...] Call Trace: <TASK> __netlink_policy_dump_write_attr+0x23d/0x990 net/netlink/policy.c:310 netlink_policy_dump_write_attr+0x22/0x30 net/netlink/policy.c:411 netlink_ack_tlv_fill net/netlink/af_netlink.c:2454 [inline] netlink_ack+0x546/0x760 net/netlink/af_netlink.c:2506 netlink_rcv_skb+0x1b7/0x240 net/netlink/af_netlink.c:2546 rtnetlink_rcv+0x18/0x20 net/core/rtnetlink.c:6109 netlink_unicast_kernel net/netlink/af_netlink.c:1319 [inline] netlink_unicast+0x5e9/0x6b0 net/netlink/af_netlink.c:1345 netlink_sendmsg+0x739/0x860 net/netlink/af_netlink.c:1921 sock_sendmsg_nosec net/socket.c:714 [inline] sock_sendmsg net/socket.c:734 [inline] ____sys_sendmsg+0x38f/0x500 net/socket.c:2482 ___sys_sendmsg net/socket.c:2536 [inline] __sys_sendmsg+0x197/0x230 net/socket.c:2565 __do_sys_sendmsg net/socket.c:2574 [inline] __se_sys_sendmsg net/socket.c:2572 [inline] __x64_sys_sendmsg+0x42/0x50 net/socket.c:2572 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x2b/0x70 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43888	In the Linux kernel, the following vulnerability has been resolved: mm: list_lru: fix UAF for memory cgroup The mem_cgroup_from_slab_obj() is supposed to be called under rcu lock or cgroup_mutex or others which could prevent returned memcg from being freed. Fix it by adding missing rcu read lock. Found by code inspection. [songmuchun@bytedance.com: only grab rcu lock when necessary, per Vlastimil] Link: https://lkml.kernel.org/r/20240801024603.1865-1-songmuchun@bytedance.com	7.8	More Details
CVE-2024-7977	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2024-44932	In the Linux kernel, the following vulnerability has been resolved: idpf: fix UAFs when destroying the queues The second tagged commit started sometimes (very rarely, but possible) throwing WARNs from net/core/page_pool.c:page_pool_disable_direct_recycling(). Turned out idpf frees interrupt vectors with embedded NAPIs *before* freeing the queues making page_pools' NAPI pointers lead to freed memory before these pools are destroyed by libeth. It's not clear whether there are other accesses to the freed vectors when destroying the queues, but anyway, we usually free queue/interrupt vectors only when the queues are destroyed and the NAPIs are guaranteed to not be referenced anywhere. Invert the allocation and freeing logic making queue/interrupt vectors be allocated first and freed last. Vectors don't require queues to be present, so this is safe. Additionally, this change allows to remove that useless queue->q_vector pointer cleanup, as vectors are still valid when freeing the queues (+ both are freed within one function, so it's not clear why nullify the pointers at all).	7.8	More Details
CVE-2024-44934	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous garbage has been collected when removing a port. What happens is: CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock call br_multicasg_gc() directly acquire lock now but free port the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000 by task syz.5.1232/9699 CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610 kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline] run_timer_base+0x111/0x190 kernel/time/timer.c:2437	7.8	More Details
CVE-2024-43873	In the Linux kernel, the following vulnerability has been resolved: vhost/vsock: always initialize seqpacket_allow There are two issues around seqpacket_allow: 1. seqpacket_allow is not initialized when socket is created. Thus if features are never set, it will be read uninitialized. 2. if VIRTIO_VSOCK_F_SEQPACKET is set and then cleared, then seqpacket_allow will not be cleared appropriately (existing apps I know about don't usually do this but it's legal and there's no way to be sure no one relies on this). To fix: - initialize seqpacket_allow after allocation - set it unconditionally in set_features	7.8	More Details
CVE-2024-43782	This openedx-translations repository contains translation files from Open edX repositories to be kept in sync with Transifex. Before moving to pulling translations from the openedx-translations repository via openedx-atlas, translations in the edx-platform repository were validated using edx-i18n-tools. This validation included protection against malformed translations and translations-based script injections. Prior to this patch, the validation implemented in the openedx-translations repository did not include the same protections. The maintainer inspected the translations in the edx-platform directory of both the main and open-release/redwood.master branches of the openedx-translations repository and found no evidence of exploited translation strings.	7.7	More Details
CVE-2024-43966	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stark Digital WP Testimonial Widget.This issue affects WP Testimonial Widget: from n/a through 3.1.	7.6	More Details
CVE-2024-36443	Swissphone DiCal-RED 4009 devices allow a remote attacker to gain read access to almost the whole file system via anonymous FTP.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7384	The AcyMailing – An Ultimate Newsletter Plugin and Marketing Automation Solution for WordPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the acym_extractArchive function in all versions up to, and including, 9.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.5	More Details
CVE-2024-42774	An Incorrect Access Control vulnerability was found in /admin/delete_room.php in Kashipara Hotel Management System v1.0, which allows an unauthenticated attacker to delete valid hotel room entries in the administrator section.	7.5	More Details
CVE-2024-43783	The Apollo Router Core is a configurable, high-performance graph router written in Rust to run a federated supergraph that uses Apollo Federation 2. Instances of the Apollo Router running versions >=1.21.0 and < 1.52.1 are impacted by a denial of service vulnerability if _all_ of the following are true: 1. The Apollo Router has been configured to support [External Coprocessing] (https://www.apollographql.com/docs/router/customizations/coprocessor). 2. The Apollo Router has been configured to send request bodies to coprocessors. This is a non-default configuration and must be configured intentionally by administrators. Instances of the Apollo Router running versions >=1.7.0 and <1.52.1 are impacted by a denial-of-service vulnerability if all of the following are true: 1. Router has been configured to use a custom-developed Native Rust Plugin. 2. The plugin accesses Request.router_request in the RouterService layer. 3. You are accumulating the body from Request.router_request into memory. If using an impacted configuration, the Router will load entire HTTP request bodies into memory without respect to other HTTP request size-limiting configurations like limits.http_max_request_bytes. This can cause the Router to be out-of-memory (OOM) terminated if a sufficiently large request is sent to the Router. By default, the Router sets limits.http_max_request_bytes to 2 MB. If you have an impacted configuration as defined above, please upgrade to at least Apollo Router 1.52.1. If you cannot upgrade, you can mitigate the denial-of-service opportunity impacting External Coprocessors by setting the coprocessor.router.request.body configuration option to false. Please note that changing this configuration option will change the information sent to any coprocessors you have configured and may impact functionality implemented by those coprocessors. If you have developed a Native Rust Plugin and cannot upgrade, you can update your plugin to either not accumulate the request body or enforce a maximum body size limit. You can also mitigate this issue by limiting HTTP body payload sizes prior to the Router (e.g., in a proxy or web application firewall appliance).	7.5	More Details
CVE-2024-43022	An issue in the downloader.php component of TOSEI online store management system v4.02, v4.03, and v4.04 allows attackers to execute a directory traversal.	7.5	More Details
CVE-2024-42772	An Incorrect Access Control vulnerability was found in /admin/rooms.php in Kashipara Hotel Management System v1.0, which allows an unauthenticated attacker to view valid hotel room entries in administrator section.	7.5	More Details
CVE-2023-29929	Buffer Overflow vulnerability found in Kemptechnologies Loadmaster before v.7.2.60.0 allows a remote attacker to casue a denial of service via the libkemplink.so, isreverse library.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43414	Apollo Federation is an architecture for declaratively composing APIs into a unified graph. Each team can own their slice of the graph independently, empowering them to deliver autonomously and incrementally. Instances of @apollo/query-planner >=2.0.0 and <2.8.5 are impacted by a denial-of-service vulnerability. @apollo/gateway versions >=2.0.0 and < 2.8.5 and Apollo Router <1.52.1 are also impacted through their use of @apollo/query-panner. If @apollo/query-planner is asked to plan a sufficiently complex query, it may loop infinitely and never complete. This results in unbounded memory consumption and either a crash or out-of-memory (OOM) termination. This issue can be triggered if you have at least one non-@key field that can be resolved by multiple subgraphs. To identify these shared fields, the schema for each subgraph must be reviewed. The mechanism to identify shared fields varies based on the version of Federation your subgraphs are using. You can check if your subgraphs are using Federation 1 or Federation 2 by reviewing their schemas. Federation 2 subgraph schemas will contain a @link directive referencing the version of Federation being used while Federation 1 subgraphs will not. For example, in a Federation 2 subgraph, you will find a line like @link(url: "https://specs.apollo.dev/federation/v2.0"). If a similar @link directive is not present in your subgraph schema, it is using Federation 1. Note that a supergraph can contain a mix of Federation 1 and Federation 2 subgraphs. This issue results from the Apollo query planner attempting to use a Number exceeding Javascript's Number.MAX_VALUE in some cases. In Javascript, Number.MAX_VALUE is (2^1024 - 2^971). When the query planner receives an inbound graphql request, it breaks the query into pieces and for each piece, generates a list of potential execution steps to solve the piece. These candidates represent the steps that the query planner will take to satisfy the pieces of the larger query. As part of normal operations, the query planner requires and calculates the number of possible query plans for the total query. That is, it needs the product of the number of query plan candidates for each piece of the query. Under normal circumstances, after generating all query plan candidates and calculating the number of all permutations, the query planner moves on to stack rank candidates and prune less-than-optimal options. In particularly complex queries, especially those where fields can be solved through multiple subgraphs, this can cause the number of all query plan permutations to balloon. In worst-case scenarios, this can end up being a number larger than Number.MAX_VALUE. In Javascript, if Number.MAX_VALUE is exceeded, Javascript represents the value as "infinity". If the count of candidates is evaluated as infinity, the component of the query planner responsible for pruning less-than-optimal query plans does not actually prune candidates, causing the query planner to evaluate many orders of magnitude more query plan candidates than necessary. This issue has been addressed in @apollo/query-planner v2.8.5, @apollo/gateway v2.8.5, and Apollo Router v1.52.1. Users are advised to upgrade. This issue can be avoided by ensuring there are no fields resolvable from multiple subgraphs. If all subgraphs are using Federation 2, you can confirm that you are not impacted by ensuring that none of your subgraph schemas use the @shareable directive. If you are using Federation 1 subgraphs, you will need to validate that there are no fields resolvable by multiple subgraphs.	7.5	More Details
CVE-2024-39776	Avtec Outpost stores sensitive information in an insecure location without proper access controls in place.	7.5	More Details
CVE-2024-8182	An Unauthenticated Denial of Service (DoS) vulnerability exists in Flowise version 1.8.2 leading to a complete crash of the instance running a vulnerable version due to improper handling of user supplied input to the "/api/v1/get-upload-file" api endpoint.	7.5	More Details
CVE-2024-45049	Hydra is a Continuous Integration service for Nix based projects. It is possible to trigger evaluations in Hydra without any authentication. Depending on the size of evaluations, this can impact the availability of systems. The problem can be fixed by applying https://github.com/NixOS/hydra/commit/f73043378907c2c7e44f633ad764c8bdd1c947d5 to any Hydra package. Users are advised to upgrade. Users unable to upgrade should deny the `/api/push` route in a reverse proxy. This also breaks the "Evaluate jobset" button in the frontend.	7.5	More Details
CVE-2024-45038	Meshtastic device firmware is a firmware for meshtastic devices to run an open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices. Meshtastic device firmware is subject to a denial of serivce vulnerability in MQTT handling, fixed in version 2.4.1 of the Meshtastic firmware and on the Meshtastic public MQTT Broker. It's strongly suggested that all users of Meshtastic, particularly those that connect to a privately hosted MQTT server, update to this or a more recent stable version right away. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2024-5991	In function MatchDomainName(), input param str is treated as a NULL terminated string despite being user provided and unchecked. Specifically, the function X509_check_host() takes in a pointer and length to check against, with no requirements that it be NULL terminated. If a caller was attempting to do a name check on a non-NULL terminated buffer, the code would read beyond the bounds of the input array until it found a NULL terminator.This issue affects wolfSSL: through 5.7.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42418	Avtec Outpost uses a default cryptographic key that can be used to decrypt sensitive information.	7.5	More Details
CVE-2024-7885	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments.	7.5	More Details
CVE-2024-45236	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a signed object containing an empty signedAttributes field. Fort accesses the set's elements without sanitizing it first. Because Fort is an RPKI Relying Party, a crash can lead to Route Origin Validation unavailability, which can lead to compromised routing.	7.5	More Details
CVE-2024-45241	A traversal vulnerability in GeneralDocs.aspx in CentralSquare CryWolf (False Alarm Management) through 2024-08-09 allows unauthenticated attackers to read files outside of the working web directory via the rpt parameter, leading to the disclosure of sensitive information.	7.5	More Details
CVE-2024-41996	Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key.	7.5	More Details
CVE-2024-43289	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in gVectors Team wpForo Forum.This issue affects wpForo Forum: from n/a through 2.3.4.	7.5	More Details
CVE-2023-49198	Mysql security vulnerability in Apache SeaTunnel. Attackers can read files on the MySQL server by modifying the information in the MySQL URL allowLoadLocalInfile=true&allowUrlInLocalInfile=true&allowLoadLocalInfileInPath=/&maxAllowedPacket=655360 This issue affects Apache SeaTunnel: 1.0.0. Users are recommended to upgrade to version [1.0.1], which fixes the issue.	7.5	More Details
CVE-2024-45239	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) an ROA or a Manifest containing a null eContent field. Fort dereferences the pointer without sanitizing it first. Because Fort is an RPKI Relying Party, a crash can lead to Route Origin Validation unavailability, which can lead to compromised routing.	7.5	More Details
CVE-2024-7401	Netskope was notified about a security gap in Netskope Client enrollment process where NSClient is using a static token “Orgkey” as authentication parameter. Since this is a static token, if leaked, cannot be rotated or revoked. A malicious actor can use this token to enroll NSClient from a customer’s tenant and impersonate a user.	7.5	More Details
CVE-2024-28077	A denial-of-service issue was discovered on certain GL-iNet devices. Some websites can detect devices exposed to the external network through DDNS, and consequently obtain the IP addresses and ports of devices that are exposed. By using special usernames and special characters (such as half parentheses or square brackets), one can call the login interface and cause the session-management program to crash, resulting in customers being unable to log into their devices. This affects MT6000 4.5.6, XE3000 4.4.5, X3000 4.4.6, MT3000 4.5.0, MT2500 4.5.0, AXT1800 4.5.0, AX1800 4.5.0, A1300 4.5.0, S200 4.1.4-0300, X750 4.3.7, SFT1200 4.3.7, MT1300 4.3.10, AR750 4.3.10, AR750S 4.3.10, AR300M 4.3.10, AR300M16 4.3.10, B1300 4.3.10, MT300N-V2 4.3.10, and XE300 4.3.16.	7.5	More Details
CVE-2024-45238	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a resource certificate containing a bit string that doesn't properly decode into a Subject Public Key. OpenSSL does not report this problem during parsing, and when compiled with OpenSSL libcrypto versions below 3, Fort recklessly dereferences the pointer. Because Fort is an RPKI Relying Party, a crash can lead to Route Origin Validation unavailability, which can lead to compromised routing.	7.5	More Details
CVE-2023-7260	Path Traversal vulnerability discovered in OpenText™ CX-E Voice, affecting all version through 22.4. The vulnerability could allow arbitrarily access files on the system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45235	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a resource certificate containing an Authority Key Identifier extension that lacks the keyIdentifier field. Fort references this pointer without sanitizing it first. Because Fort is an RPKI Relying Party, a crash can lead to Route Origin Validation unavailability, which can lead to compromised routing.	7.5	More Details
CVE-2024-43410	Russh is a Rust SSH client & server library. Allocating an untrusted amount of memory allows any unauthenticated user to OOM a russh server. An SSH packet consists of a 4-byte big-endian length, followed by a byte stream of this length. After parsing and potentially decrypting the 4-byte length, russh allocates enough memory for this bytestream, as a performance optimization to avoid reallocations later. But this length is entirely untrusted and can be set to any value by the client, causing this much memory to be allocated, which will cause the process to OOM within a few such requests. This vulnerability is fixed in 0.44.1.	7.5	More Details
CVE-2024-42490	authentik is an open-source Identity Provider. Several API endpoints can be accessed by users without correct authentication/authorization. The main API endpoints affected by this are /api/v3/crypto/certificatekeypairs/<uuid>/view_certificate/, /api/v3/crypto/certificatekeypairs/<uuid>/view_private_key/, and /api/v3/.../used_by/. Note that all of the affected API endpoints require the knowledge of the ID of an object, which especially for certificates is not accessible to an unprivileged user. Additionally the IDs for most objects are UUIDv4, meaning they are not easily guessable/enumerable. authentik 2024.4.4, 2024.6.4 and 2024.8.0 fix this issue.	7.5	More Details
CVE-2024-45234	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) an ROA or a Manifest containing a signedAttrs encoded in non-canonical form. This bypasses Fort's BER decoder, reaching a point in the code that panics when faced with data not encoded in DER. Because Fort is an RPKI Relying Party, a panic can lead to Route Origin Validation unavailability, which can lead to compromised routing.	7.5	More Details
CVE-2024-43477	Improper access control in Decentralized Identity Services resulted in a vulnerability that allows an unauthenticated attacker to disable Verifiable ID's on another tenant.	7.5	More Details
CVE-2024-45240	The TikTok (aka com.zhiliaoapp.musically) application before 34.5.5 for Android allows the takeover of Lynxview JavaScript interfaces via deeplink traversal (in the application's exposed WebView). (On Android 12 and later, this is only exploitable by third-party applications.)	7.4	More Details
CVE-2024-8081	A vulnerability classified as critical was found in itsourcecode Payroll Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-41176	The MPD package included in TwinCAT/BSD allows an authenticated, low-privileged local attacker to induce a Denial-of-Service (DoS) condition on the daemon and execute code in the context of user “root” via a crafted HTTP request.	7.3	More Details
CVE-2024-8168	A vulnerability was found in code-projects Online Bus Reservation Site 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-44386	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the function fromSetIpBind.	7.3	More Details
CVE-2024-8217	A vulnerability has been found in SourceCodester E-Commerce Website 1.0 and classified as critical. This vulnerability affects unknown code of the file /Admin/registration.php. The manipulation of the argument fname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8169	A vulnerability was found in code-projects Online Quiz Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file signupuser.php. The manipulation of the argument lid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8173	A vulnerability, which was classified as critical, was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file /login.php of the component Login Page. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41174	The IPC-Diagnostics package in TwinCAT/BSD is susceptible to improper input neutralization by a low-privileged local attacker.	7.3	More Details
CVE-2024-8219	A vulnerability was found in code-projects Responsive Hotel Site 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument name/phone/email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2020-11850	Improper Input Validation vulnerability in OpenText Self Service Password Reset allows Cross-Site Scripting (XSS). This issue affects Self Service Password Reset before 4.5.0.2 and 4.4.0.6	7.3	More Details
CVE-2024-38305	Dell SupportAssist for Home PCs Installer exe version 4.0.3 contains a privilege escalation vulnerability in the installer. A local low-privileged authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary executables on the operating system with elevated privileges.	7.3	More Details
CVE-2024-8167	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file /forget.php. The manipulation of the argument email/mobile leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8086	A vulnerability has been found in SourceCodester E-Commerce System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ecommerce/admin/login.php of the component Admin Login. The manipulation of the argument user_email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8218	A vulnerability was found in code-projects Online Quiz Site 1.0 and classified as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument loginid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-39717	The Versa Director GUI provides an option to customize the look and feel of the user interface. This option is only available for a user logged with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin. (Tenant level users do not have this privilege). The “Change Favicon” (Favorite Icon) option can be mis-used to upload a malicious file ending with .png extension to masquerade as image file. This is possible only after a user with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin has successfully authenticated and logged in.	7.2	More Details
CVE-2024-42523	publiccms V4.0.202302.e and before is vulnerable to Any File Upload via publiccms/admin/cmsTemplate/saveMetaData	7.2	More Details
CVE-2024-6632	A vulnerability exists in FileCatalyst Workflow whereby a field accessible to the super admin can be used to perform an SQL injection attack which can lead to a loss of confidentiality, integrity, and availability.	7.2	More Details
CVE-2024-42767	Kashipara Hotel Management System v1.0 is vulnerable to Unrestricted File Upload RCE via /admin/add_room_controller.php.	7.2	More Details
CVE-2024-7134	The LiquidPoll – Polls, Surveys, NPS and Feedback Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘form_data’ parameter in all versions up to, and including, 3.3.78 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-42776	Kashipara Hotel Management System v1.0 is vulnerable to Incorrect Access Control via /admin/users.php.	7.2	More Details
CVE-2024-7351	The Simple Job Board plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.12.3 via deserialization of untrusted input when editing job applications. This makes it possible for authenticated attackers, with Editor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	7.2	More Details
CVE-2024-42636	DedeCMS V5.7.115 has a command execution vulnerability via file_manage_view.php?fmdo=newfile&activepath.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45187	Guest users in the Mage AI framework that remain logged in after their accounts are deleted, are mistakenly given high privileges and specifically given access to remotely execute arbitrary code through the Mage AI terminal server	7.1	More Details
CVE-2024-43255	Cross-Site Request Forgery (CSRF) vulnerability in Stormhill Media MyBookTable Bookstore allows Cross-Site Scripting (XSS).This issue affects MyBookTable Bookstore: from n/a through 3.3.9.	7.1	More Details
CVE-2022-48871	In the Linux kernel, the following vulnerability has been resolved: tty: serial: qcom-geni-serial: fix slab-out-of-bounds on RX FIFO buffer Driver's probe allocates memory for RX FIFO (port->rx_fifo) based on default RX FIFO depth, e.g. 16. Later during serial startup the qcom_geni_serial_port_setup() updates the RX FIFO depth (port->rx_fifo_depth) to match real device capabilities, e.g. to 32. The RX UART handle code will read "port->rx_fifo_depth" number of words into "port->rx_fifo" buffer, thus exceeding the bounds. This can be observed in certain configurations with Qualcomm Bluetooth HCI UART device and KASAN: Bluetooth: hci0: QCA Product ID :0x00000010 Bluetooth: hci0: QCA SOC Version :0x400a0200 Bluetooth: hci0: QCA ROM Version :0x00000200 Bluetooth: hci0: QCA Patch Version:0x00000d2b Bluetooth: hci0: QCA controller version 0x02000200 Bluetooth: hci0: QCA Downloading qca/htbtfw20.tlv bluetooth hci0: Direct firmware load for qca/htbtfw20.tlv failed with error -2 Bluetooth: hci0: QCA Failed to request file: qca/htbtfw20.tlv (-2) Bluetooth: hci0: QCA Failed to download patch (-2) == BUG: KASAN: slab-out-of-bounds in handle_rx_uart+0xa8/0x18c Write of size 4 at addr ffff279347d578c0 by task swapper/0/0 CPU: 0 PID: 0 Comm: swapper/0 Not tainted 6.1.0-rt5-00350-gb2450b7e00be-dirty #26 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: dump_backtrace.part.0+0xe0/0xf0 show_stack+0x18/0x40 dump_stack_lvl+0x8c/0xb8 print_report+0x188/0x488 kasan_report+0xb4/0x100 __asan_store4+0x80/0xa4 handle_rx_uart+0xa8/0x18c qcom_geni_serial_handle_rx+0x84/0x9c qcom_geni_serial_isr+0x24c/0x760 __handle_irq_event_percpu+0x108/0x500 handle_irq_event+0x6c/0x110 handle_fasteoi_irq+0x138/0x2cc generic_handle_domain_irq+0x48/0x64 If the RX FIFO depth changes after probe, be sure to resize the buffer.	7.1	More Details
CVE-2022-48881	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd: Fix refcount leak in amd_pmc_probe pci_get_domain_bus_and_slot() takes reference, the caller should release the reference by calling pci_dev_put() after use. Call pci_dev_put() in the error path to fix this.	7.1	More Details
CVE-2024-43301	Cross-Site Request Forgery (CSRF) vulnerability in Fonts Plugin Fonts allows Stored XSS.This issue affects Fonts: from n/a through 3.7.7.	7.1	More Details
CVE-2023-22576	Dell Repository Manager version 3.4.2 and earlier, contain a Local Privilege Escalation Vulnerability in Installation module. A local low privileged attacker may potentially exploit this vulnerability leading to the execution of arbitrary executable on the operating system with high privileges using the existing vulnerability in operating system. Exploitation may lead to unavailability of the service.	7.0	More Details
CVE-2022-48872	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix use-after-free race condition for maps It is possible that in between calling fastrpc_map_get() until map->fl->lock is taken in fastrpc_free_map(), another thread can call fastrpc_map_lookup() and get a reference to a map that is about to be deleted. Rewrite fastrpc_map_get() to only increase the reference count of a map if it's non-zero. Propagate this to callers so they can know if a map is about to be deleted. Fixes this warning: refcount_t: addition on 0; use-after-free. WARNING: CPU: 5 PID: 10100 at lib/refcount.c:25 refcount_warn_saturate ... Call trace: refcount_warn_saturate [fastrpc_map_get inlined] [fastrpc_map_lookup inlined] fastrpc_map_create fastrpc_internal_invoke fastrpc_device_ioctl __arm64_sys_ioctl invoke_syscall	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43882	In the Linux kernel, the following vulnerability has been resolved: exec: Fix ToCToU between perm check and set-uid/gid usage When opening a file for exec via do_filp_open(), permission checking is done against the file's metadata at that moment, and on success, a file pointer is passed back. Much later in the execve() code path, the file metadata (specifically mode, uid, and gid) is used to determine if/how to set the uid and gid. However, those values may have changed since the permissions check, meaning the execution may gain unintended privileges. For example, if a file could change permissions from executable and not set-id: ---------x 1 root root 16048 Aug 7 13:16 target to set-id and non-executable: ---S------ 1 root root 16048 Aug 7 13:16 target it is possible to gain root privileges when execution should have been disallowed. While this race condition is rare in real-world scenarios, it has been observed (and proven exploitable) when package managers are updating the setuid bits of installed programs. Such files start with being world-executable but then are adjusted to be group-exec with a set-uid bit. For example, "chmod o-x,u+s target" makes "target" executable only by uid "root" and gid "cdrom", while also becoming setuid-root: -rwxr-xr-x 1 root cdrom 16048 Aug 7 13:16 target becomes: -rwsr-xr-- 1 root cdrom 16048 Aug 7 13:16 target But racing the chmod means users without group "cdrom" membership can get the permission to execute "target" just before the chmod, and when the chmod finishes, the exec reaches brpm_fill_uid(), and performs the setuid to root, violating the expressed authorization of "only cdrom group members can setuid to root". Re-check that we still have execute permissions in case the metadata has changed. It would be better to keep a copy from the perm-check time, but until we can do that refactoring, the least-bad option is to do a full inode_permission() call (under inode lock). It is understood that this is safe against dead-locks, but hardly optimal.	7.0	More Details
CVE-2024-42768	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Hotel Management System v1.0 via /admin/delete_room.php.	6.8	More Details
CVE-2024-36440	An issue was discovered on Swissphone DiCal-RED 4009 devices. An attacker with access to the file /etc/deviceconfig may recover the administrative device password via password-cracking methods, because unsalted MD5 is used.	6.8	More Details
CVE-2024-41675	CKAN is an open-source data management system for powering data hubs and data portals. The Datatables view plugin did not properly escape record data coming from the DataStore, leading to a potential XSS vector. Sites running CKAN >= 2.7.0 with the datatables_view plugin activated. This is a plugin included in CKAN core, that not activated by default but it is widely used to preview tabular data. This vulnerability has been fixed in CKAN 2.10.5 and 2.11.0.	6.8	More Details
CVE-2022-43915	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with privileged access to execute commands in a running Pod to elevate their user privileges.	6.8	More Details
CVE-2024-44387	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the functino formWrlExtraGet.	6.5	More Details
CVE-2024-45188	Mage AI allows remote users with the "Viewer" role to leak arbitrary files from the Mage server due to a path traversal in the "File Content" request	6.5	More Details
CVE-2024-7602	Logsign Unified SecOps Platform Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-25027.	6.5	More Details
CVE-2024-7032	The Smart Online Order for Clover plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'moo_deactivateAndClean' function in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to deactivate the plugin and drop all plugin tables from the database.	6.5	More Details
CVE-2024-8041	A Denial of Service (DoS) issue has been discovered in GitLab CE/EE affecting all versions prior to 17.1.6, 17.2 prior to 17.2.4, and 17.3 prior to 17.3.1. A denial of service could occur upon importing a maliciously crafted repository using the GitHub importer.	6.5	More Details
CVE-2024-43257	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Nouthemes Leopard - WordPress offload media.This issue affects Leopard - WordPress offload media: from n/a through 2.0.36.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40395	An Insecure Direct Object Reference (IDOR) in PTC ThingWorx v9.5.0 allows attackers to view sensitive information, including PII, regardless of access level.	6.5	More Details
CVE-2024-43251	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Bit Apps Bit Form Pro.This issue affects Bit Form Pro: from n/a through 2.6.4.	6.5	More Details
CVE-2024-20417	Multiple vulnerabilities in the REST API of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct blind SQL injection attacks. These vulnerabilities are due to insufficient validation of user-supplied input in REST API calls. An attacker could exploit these vulnerabilities by sending crafted input to an affected device. A successful exploit could allow the attacker to view or modify data on the affected device.	6.5	More Details
CVE-2024-20466	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to improper enforcement of administrative privilege levels for high-value sensitive data. An attacker with read-only Administrator privileges for the web-based management interface on an affected device could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system.	6.5	More Details
CVE-2024-43806	Rustix is a set of safe Rust bindings to POSIX-ish APIs. When using `rustix::fs::Dir` using the `linux_raw` backend, it's possible for the iterator to "get stuck" when an IO error is encountered. Combined with a memory over-allocation issue in `rustix::fs::Dir::read_more`, this can cause quick and unbounded memory explosion (gigabytes in a few seconds if used on a hot path) and eventually lead to an OOM crash of the application. The symptoms were initially discovered in https://github.com/imsnif/bandwhich/issues/284. That post has lots of details of our investigation. Full details can be read on the GHSA-c827-hfw6-qwvm repo advisory. If a program tries to access a directory with its file descriptor after the file has been unlinked (or any other action that leaves the `Dir` iterator in the stuck state), and the implementation does not break after seeing an error, it can cause a memory explosion. As an example, Linux's various virtual file systems (e.g. `/proc`, `/sys`) can contain directories that spontaneously pop in and out of existence. Attempting to iterate over them using `rustix::fs::Dir` directly or indirectly (e.g. with the `procfs` crate) can trigger this fault condition if the implementation decides to continue on errors. An attacker knowledgeable about the implementation details of a vulnerable target can therefore try to trigger this fault condition via any one or a combination of several available APIs. If successful, the application host will quickly run out of memory, after which the application will likely be terminated by an OOM killer, leading to denial of service. This issue has been addressed in release versions 0.35.15, 0.36.16, 0.37.25, and 0.38.19. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2024-20486	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the targeted user.	6.5	More Details
CVE-2024-8158	A bug in the 9p authentication implementation within lib9p allows an attacker with an existing valid user within the configured auth server to impersonate any other valid filesystem user. This is due to lib9p not properly verifying that the uname given in the Tauth and Tattach 9p messages matches the client UID returned from the factotum authentication handshake. The only filesystem making use of these functions within the base 9front systems is the experimental hjfs disk filesystem, other disk filesystems (cwfs and gefs) are not affected by this bug. This bug was inherited from Plan 9 and is present in all versions of 9front and is remedied fully in commit 9645ae07eb66a59015e3e118d0024790c37400da.	6.5	More Details
CVE-2024-35151	IBM OpenPages with Watson 8.3 and 9.0 could allow authenticated users access to sensitive information through improper authorization controls on APIs.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42364	Homepage is a highly customizable homepage with Docker and service API integrations. The default setup of homepage 0.9.1 is vulnerable to DNS rebinding. Homepage is setup without certificate and authentication by default, leaving it to vulnerable to DNS rebinding. In this attack, an attacker will ask a user to visit his/her website. The attacker website will then change the DNS records of their domain from their IP address to the internal IP address of the homepage instance. To tell which IP addresses are valid, we can rebind a subdomain to each IP address we want to check, and see if there is a response. Once potential candidates have been found, the attacker can launch the attack by reading the response of the webserver after the IP address has changed. When the attacker domain is fetched, the response will be from the homepage instance, not the attacker website, because the IP address has been changed. Due to a lack of authentication, a user's private information such as API keys (fixed after first report) and other private information can then be extracted by the attacker website.	6.5	More Details
CVE-2023-26315	The Xiaomi router AX9000 has a post-authentication command injection vulnerability. This vulnerability is caused by the lack of input filtering, allowing an attacker to exploit it to obtain root access to the device.	6.5	More Details
CVE-2024-42056	Retool (self-hosted enterprise) through 3.40.0 inserts resource authentication credentials into sent data. Credentials for users with "Use" permissions can be discovered (by an authenticated attacker) via the /api/resources endpoint. The earliest affected version is 3.18.1.	6.5	More Details
CVE-2024-45190	Mage AI allows remote users with the "Viewer" role to leak arbitrary files from the Mage server due to a path traversal in the "Pipeline Interaction" request	6.5	More Details
CVE-2024-45189	Mage AI allows remote users with the "Viewer" role to leak arbitrary files from the Mage server due to a path traversal in the "Git Content" request	6.5	More Details
CVE-2024-6789	A path traversal issue in API endpoint in M-Files Server before version 24.8.13981.0 and LTS 24.2.13421.15 SR2 and LTS 23.8.12892.0 SR6 allows authenticated user to read files	6.5	More Details
CVE-2024-7778	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.10.36 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-5502	The Piotnet Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Accordion, Dual Heading, and Vertical Timeline widgets in all versions up to, and including, 2.4.30 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-2024-6870	The Responsive Lightbox & Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via file uploads in all versions up to, and including, 2.4.7 due to insufficient input sanitization and output escaping affecting the rl_upload_image AJAX endpoint. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the 3gp2 file.	6.4	More Details
CVE-2024-7110	An issue was discovered in GitLab EE affecting all versions starting 17.0 to 17.1.6, 17.2 prior to 17.2.4, and 17.3 prior to 17.3.1 allows an attacker to execute arbitrary command in a victim's pipeline through prompt injection.	6.4	More Details
CVE-2024-5583	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the carousel_direction parameter of testimonials widget in all versions up to, and including, 5.6.2 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-2024-45037	The AWS Cloud Development Kit (CDK) is an open-source framework for defining cloud infrastructure using code. Customers use it to create their own applications which are converted to AWS CloudFormation templates during deployment to a customer's AWS account. CDK contains pre-built components called "constructs" that are higher-level abstractions providing defaults and best practices. This approach enables developers to use familiar programming languages to define complex cloud infrastructure more efficiently than writing raw CloudFormation templates. We identified an issue in AWS Cloud Development Kit (CDK) which, under certain conditions, can result in granting authenticated Amazon Cognito users broader than intended access. Specifically, if a CDK application uses the "RestApi" construct with "CognitoUserPoolAuthorizer" as the authorizer and uses authorization scopes to limit access. This issue does not affect the availability of the specific API resources. Authenticated Cognito users may gain unintended access to protected API resources or methods, leading to potential data disclosure, and modification issues. Impacted versions: >=2.142.0;<=2.148.0. A patch is included in CDK versions >=2.148.1. Users are advised to upgrade their AWS CDK version to 2.148.1 or newer and re-deploy their application(s) to address this issue.	6.4	More Details
CVE-2024-8105	A vulnerability related to the use an insecure Platform Key (PK) has been discovered. An attacker with the compromised PK private key can create malicious UEFI software that is signed with a trusted key that has been compromised.	6.4	More Details
CVE-2024-2254	The RT Easy Builder – Advanced addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6804	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-7304	The Ninja Tables – Easiest Data Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 5.0.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-8046	The Logo Showcase Ultimate – Logo Carousel, Logo Slider & Logo Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-7791	The 140+ Widgets I Xpro Addons For Elementor – FREE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'arrow' parameter within the Post Grid widget in all versions up to, and including, 1.4.4.3 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-2024-8207	In certain highly specific configurations of the host system and MongoDB server binary installation on Linux Operating Systems, it may be possible for a unintended actor with host-level access to cause the MongoDB Server binary to load unintended actor-controlled shared libraries when the server binary is started, potentially resulting in the unintended actor gaining full control over the MongoDB server process. This issue affects MongoDB Server v5.0 versions prior to 5.0.14 and MongoDB Server v6.0 versions prior to 6.0.3. Required Configuration: Only environments with Linux as the underlying operating system is affected by this issue	6.4	More Details
CVE-2024-7629	The Responsive video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's video settings function in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires responsive videos to be enabled for posts.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43788	Webpack is a module bundler. Its main purpose is to bundle JavaScript files for usage in a browser, yet it is also capable of transforming, bundling, or packaging just about any resource or asset. The webpack developers have discovered a DOM Clobbering vulnerability in Webpack's `AutoPublicPathRuntimeModule`. The DOM Clobbering gadget in the module can lead to cross-site scripting (XSS) in web pages where scriptless attacker-controlled HTML elements (e.g., an `img` tag with an unsanitized `name` attribute) are present. Real-world exploitation of this gadget has been observed in the Canvas LMS which allows a XSS attack to happen through a javascript code compiled by Webpack (the vulnerable part is from Webpack). DOM Clobbering is a type of code-reuse attack where the attacker first embeds a piece of non-script, seemingly benign HTML markups in the webpage (e.g. through a post or comment) and leverages the gadgets (pieces of js code) living in the existing javascript code to transform it into executable code. This vulnerability can lead to cross-site scripting (XSS) on websites that include Webpack-generated files and allow users to inject certain scriptless HTML tags with improperly sanitized name or id attributes. This issue has been addressed in release version 5.94.0. All users are advised to upgrade. There are no known workarounds for this issue.	6.4	More Details
CVE-2024-8210	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8171	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. This vulnerability affects unknown code of the file staffcatedit.php. The manipulation of the argument title 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-2024-8211	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8212	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8213	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8214	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8220	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file staffedit.php. The manipulation of the argument id/stafftype/address/fullname/phonenumber/salary leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8221	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8222	A vulnerability classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file /admin/?page=musics/manage_music. 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-2024-8223	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. This vulnerability affects unknown code of the file /classes/Master.php?f=delete_category. 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-2024-8075	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg. The manipulation leads to os command injection. The attack can be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-8077	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been classified as critical. This affects the function setTracerouteCfg. The manipulation leads to os command injection. It is possible to initiate the attack remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-41150	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter Plus: through 14800.	6.3	More Details
CVE-2024-8087	A vulnerability was found in SourceCodester E-Commerce System 1.0 and classified as critical. This issue affects some unknown processing of the file /ecommerce/popup_Item.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.	6.3	More Details
CVE-2024-38207	Microsoft Edge (HTML-based) Memory Corruption Vulnerability	6.3	More Details
CVE-2024-8127	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8128	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8129	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-38807	Applications that use spring-boot-loader or spring-boot-loader-classic and contain custom code that performs signature verification of nested jar files may be vulnerable to signature forgery where content that appears to have been signed by one signer has, in fact, been signed by another.	6.3	More Details
CVE-2024-8130	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8131	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8133	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8134	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-42789	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/music/controller.php?page=test" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via the "page" parameter.	6.3	More Details
CVE-2024-8135	A vulnerability classified as critical has been found in Go-Tribe gotribe up to cd3ccd32cd77852c9ea73f986eaf8c301cfb6310. Affected is the function Sign of the file pkg/token/token.go. The manipulation of the argument config.key leads to hard-coded credentials. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as 4fb9b9e80a2beedd09d9fde4b9cf5bd510baf18f. It is recommended to apply a patch to fix this issue.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8138	A vulnerability, which was classified as critical, was found in code-projects Pharmacy Management System 1.0. Affected is the function editManager of the file /index.php?action=editManager of the component Parameter Handler. The manipulation of the argument id as part of String leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	6.3	More Details
CVE-2024-8083	A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file /php-ocls/classes/Master.php?f=pay_order. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8139	A vulnerability has been found in itsourcecode E-Commerce Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file search_list.php. The manipulation of the argument user leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8146	A vulnerability has been found in code-projects Pharmacy Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /index.php?action=editSalesman. 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-2024-8080	A vulnerability classified as critical has been found in SourceCodester Online Health Care System 1.0. Affected is an unknown function of the file search.php. The manipulation of the argument f_name with the input 1%' or 1=1) UNION SELECT 1,2,3,4,5,database(),7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23# as part of string leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8147	A vulnerability was found in code-projects Pharmacy Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /index.php?action=editPharmacist. 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.	6.3	More Details
CVE-2024-8164	A vulnerability, which was classified as critical, has been found in Chengdu Everbrite Network Technology BeikeShop up to 1.5.5. Affected by this issue is the function rename of the file /Admin/Http/Controllers/FileManagerController.php. The manipulation of the argument new_name leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-8132	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-8089	A vulnerability was found in SourceCodester E-Commerce System 1.0. It has been classified as critical. Affected is an unknown function of the file /ecommerce/admin/products/controller.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8023	A vulnerability classified as critical has been found in chillzhuang SpringBlade 4.1.0. Affected is an unknown function of the file /api/blade-system/menu/list?updatexml. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-41572	Learning with Texts (LWT) 2.0.3 is vulnerable to Cross Site Scripting (XSS). The application has a specific function that does not filter special characters in URL parameters. Remote attackers can inject JavaScript code without authorization. Exploiting this vulnerability, attackers can steal user credentials or execute actions such as injecting malicious scripts or redirecting users to malicious sites.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38859	XSS in the view page with the SLA column configured in Checkmk versions prior to 2.3.0p14, 2.2.0p33, 2.1.0p47 and 2.0.0 (EOL) allowed malicious users to execute arbitrary scripts by injecting HTML elements into the SLA column title. These scripts could be executed when the view page was cloned by other users.	6.1	More Details
CVE-2024-42761	A Stored Cross Site Scripting (XSS) vulnerability was found in "/admin_schedule.php" in Kashipara Bus Ticket Reservation System v1.0, which allows remote attackers to execute arbitrary code via scheduleDurationPHP parameter.	6.1	More Details
CVE-2024-44795	A cross-site scripting (XSS) vulnerability in the component /login/disabled.php of Gazelle commit 63b3370 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter.	6.1	More Details
CVE-2024-44794	A cross-site scripting (XSS) vulnerability in the component /master/auth/OnedriveRedirect.php of PicUploader commit fcf82ea allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the error_description parameter.	6.1	More Details
CVE-2024-44793	A cross-site scripting (XSS) vulnerability in the component /managers/multiple_freeleech.php of Gazelle commit 63b3370 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the torrents parameter.	6.1	More Details
CVE-2024-42906	TestLink before v.1.9.20 is vulnerable to Cross Site Scripting (XSS) via the pop-up on upload file. When uploading a file, the XSS payload can be entered into the file name.	6.1	More Details
CVE-2024-38208	Microsoft Edge for Android Spoofing Vulnerability	6.1	More Details
CVE-2024-42818	A cross-site scripting (XSS) vulnerability in the Config-Create function of fastapi-admin pro v0.1.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Name parameter.	6.1	More Details
CVE-2024-42816	A cross-site scripting (XSS) vulnerability in the Create Product function of fastapi-admin pro v0.1.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Name parameter.	6.1	More Details
CVE-2024-6715	The Ditty WordPress plugin before 3.1.46 re-introduced a previously fixed security issue (https://wpscan.com/vulnerability/80a9eb3a-2cb1-4844-9004-ba2554b2d46c/) in v3.1.39	6.1	More Details
CVE-2024-42788	A Stored Cross Site Scripting (XSS) vulnerability was found in "/music/ajax.php?action=save_music" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via "title" & "artist" parameter fields.	6.1	More Details
CVE-2024-42787	A Stored Cross Site Scripting (XSS) vulnerability was found in "/music/ajax.php?action=save_playlist" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via "title" & "description" parameter fields.	6.1	More Details
CVE-2024-39097	There is an Open Redirect vulnerability in Gnuboard v6.0.4 and below via the `url` parameter in login path.	6.1	More Details
CVE-2023-6987	The String locator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'sql-column' parameter in all versions up to, and including, 2.6.5 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. This required WP_DEBUG to be enabled in order to be exploited.	6.1	More Details
CVE-2024-44797	A cross-site scripting (XSS) vulnerability in the component /managers/enable_requests.php of Gazelle commit 63b3370 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the view parameter.	6.1	More Details
CVE-2024-42769	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/core/signup_user.php " of Kashipara Hotel Management System v1.0, which allows remote attackers to execute arbitrary code via "user_fname" and "user_lname" parameters.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43794	OpenSearch Dashboards Security Plugin adds a configuration management UI for the OpenSearch Security features to OpenSearch Dashboards. Improper validation of the nextUrl parameter can lead to external redirect on login to OpenSearch-Dashboards for specially crafted parameters. A patch is available in 1.3.19 and 2.16.0 for this issue.	6.1	More Details
CVE-2024-7313	The Shield Security WordPress plugin before 20.0.6 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.	6.1	More Details
CVE-2024-42852	Cross Site Scripting vulnerability in AcuToWeb server v.10.5.0.7577C8b allows a remote attacker to execute arbitrary code via the index.php component.	6.1	More Details
CVE-2024-7647	The OTA Sync Booking Engine Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.7. This is due to missing or incorrect nonce validation on the otasync_widget_settings_fnc() function. This makes it possible for unauthenticated attackers to update the plugin's settings and inject malicious scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-6339	The Phlox PRO theme for WordPress is vulnerable to Reflected Cross-Site Scripting via search parameters in all versions up to, and including, 5.16.4 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-2024-7090	The LH Add Media From Url plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'lh_add_media_from_url-file_url' parameter in all versions up to, and including, 1.23 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-43407	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A potential vulnerability has been discovered in CKEditor 4 Code Snippet GeSHi plugin. The vulnerability allowed a reflected XSS attack by exploiting a flaw in the GeSHi syntax highlighter library hosted by the victim. The GeSHi library was included as a vendor dependency in CKEditor 4 source files. In a specific scenario, an attacker could craft a malicious script that could be executed by sending a request to the GeSHi library hosted on a PHP web server. The GeSHi library is no longer actively maintained. Due to the lack of ongoing support and updates, potential security vulnerabilities have been identified with its continued use. To mitigate these risks and enhance the overall security of the CKEditor 4, we have decided to completely remove the GeSHi library as a dependency. This change aims to maintain a secure environment and reduce the risk of any security incidents related to outdated or unsupported software. The fix is be available in version 4.25.0-lts.	6.1	More Details
CVE-2024-37392	A stored Cross-Site Scripting (XSS) vulnerability has been identified in SMSEagle software version < 6.0. The vulnerability arises because the application did not properly sanitize user input in the SMS messages in the inbox. This could allow an attacker to inject malicious JavaScript code into an SMS message, which gets executed when the SMS is viewed and specially interacted in web-GUI.	6.1	More Details
CVE-2024-41937	Apache Airflow, versions before 2.10.0, have a vulnerability that allows the developer of a malicious provider to execute a cross-site scripting attack when clicking on a provider documentation link. This would require the provider to be installed on the web server and the user to click the provider link. Users should upgrade to 2.10.0 or later, which fixes this vulnerability.	6.1	More Details
CVE-2024-20488	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2024-44796	A cross-site scripting (XSS) vulnerability in the component /auth/AzureRedirect.php of PicUploader commit fcf82ea allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the error_description parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42497	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to properly enforce permissions which allows a user with systems manager role with read-only access to teams to perform write operations on teams.	6.0	More Details
CVE-2024-43967	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Stark Digital WP Testimonial Widget allows Stored XSS.This issue affects WP Testimonial Widget: from n/a through 3.1.	5.9	More Details
CVE-2024-39745	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details
CVE-2024-43398	REXML is an XML toolkit for Ruby. The REXML gem before 3.3.6 has a DoS vulnerability when it parses an XML that has many deep elements that have same local name attributes. If you need to parse untrusted XMLs with tree parser API like REXML::Document.new, you may be impacted to this vulnerability. If you use other parser APIs such as stream parser API and SAX2 parser API, this vulnerability is not affected. The REXML gem 3.3.6 or later include the patch to fix the vulnerability.	5.9	More Details
CVE-2024-39746	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2024-7608	An authenticated user can access the restricted files from NX, EX, FX, AX, IVX and CMS using path traversal.	5.9	More Details
CVE-2024-6502	An issue was discovered in GitLab CE/EE affecting all versions starting from 8.2 prior to 17.1.6 starting from 17.2 prior to 17.2.4, and starting from 17.3 prior to 17.3.1, which allows an attacker to create a branch with the same name as a deleted tag.	5.7	More Details
CVE-2024-7651	The App Builder – Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to limited SQL Injection via the ‘app-builder-search’ parameter in all versions up to, and including, 4.2.6 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.	5.6	More Details
CVE-2024-43905	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix the null pointer dereference for vega10_hwmgr Check return value and conduct null pointer handling to avoid null pointer dereference.	5.5	More Details
CVE-2024-43896	In the Linux kernel, the following vulnerability has been resolved: ASoC: cs-amp-lib: Fix NULL pointer crash if efi.get_variable is NULL Call efi_rt_services_supported() to check that efi.get_variable exists before calling it.	5.5	More Details
CVE-2024-43908	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it	5.5	More Details
CVE-2024-43890	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix overflow in get_free_elt() "tracing_map->next_elt" in get_free_elt() is at risk of overflowing. Once it overflows, new elements can still be inserted into the tracing_map even though the maximum number of elements (`max_elts`) has been reached. Continuing to insert elements after the overflow could result in the tracing_map containing "tracing_map->max_size" elements, leaving no empty entries. If any attempt is made to insert an element into a full tracing_map using `__tracing_map_insert()`, it will cause an infinite loop with preemption disabled, leading to a CPU hang problem. Fix this by preventing any further increments to "tracing_map->next_elt" once it reaches "tracing_map->max_elt".	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43893	In the Linux kernel, the following vulnerability has been resolved: serial: core: check uartclk for zero to avoid divide by zero Calling ioctl TIOCSSERIAL with an invalid baud_base can result in uartclk being zero, which will result in a divide by zero error in uart_get_divisor(). The check for uartclk being zero in uart_set_info() needs to be done before other settings are made as subsequent calls to ioctl TIOCSSERIAL for the same port would be impacted if the uartclk check was done where uartclk gets set. Oops: divide error: 0000 PREEMPT SMP KASAN PTI RIP: 0010:uart_get_divisor (drivers/tty/serial/serial_core.c:580) Call Trace: <TASK> serial8250_get_divisor (drivers/tty/serial/8250/8250_port.c:2576 drivers/tty/serial/8250/8250_port.c:2589) serial8250_do_set_termios (drivers/tty/serial/8250/8250_port.c:502 drivers/tty/serial/8250/8250_port.c:2741) serial8250_set_termios (drivers/tty/serial/8250/8250_port.c:2862) uart_change_line_settings (./include/linux/spinlock.h:376 ./include/linux/serial_core.h:608 drivers/tty/serial/serial_core.c:222) uart_port_startup (drivers/tty/serial/serial_core.c:342) uart_startup (drivers/tty/serial/serial_core.c:368) uart_set_info (drivers/tty/serial/serial_core.c:1034) uart_set_info_user (drivers/tty/serial/serial_core.c:1059) tty_set_serial (drivers/tty/tty_io.c:2637) tty_ioctl (drivers/tty/tty_io.c:2647 drivers/tty/tty_io.c:2791) __x64_sys_ioctl (fs/ioctl.c:52 fs/ioctl.c:907 fs/ioctl.c:893 fs/ioctl.c:893) do_syscall_64 (arch/x86/entry/common.c:52 (discriminator 1) arch/x86/entry/common.c:83 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Rule: add	5.5	More Details
CVE-2024-43894	In the Linux kernel, the following vulnerability has been resolved: drm/client: fix null pointer dereference in drm_client_modeset_probe In drm_client_modeset_probe(), the return value of drm_mode_duplicate() is assigned to modeset->mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	5.5	More Details
CVE-2024-43895	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip Recompute DSC Params if no Stream on Link [why] Encounter NULL pointer dereference uner mst + dsc setup. BUG: kernel NULL pointer dereference, address: 0000000000000008 PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 4 PID: 917 Comm: sway Not tainted 6.3.9-arch1-1 #1 124dc55df4f5272ccb409f39ef4872fc2b3376a2 Hardware name: LENOVO 20NKS01Y00/20NKS01Y00, BIOS R12ET61W(1.31) 07/28/2022 RIP: 0010:drm_dp_atomic_find_time_slots+0x5e/0x260 [drm_display_helper] Code: 01 00 00 48 8b 85 60 05 00 00 48 63 80 88 00 00 00 3b 43 28 0f 8d 2e 01 00 00 48 8b 53 30 48 8d 04 80 48 8d 04 c2 48 8b 40 18 <48> 8> RSP: 0018:ffff960cc2df77d8 EFLAGS: 00010293 RAX: 0000000000000000 RBX: ffff8afb87e81280 RCX: 0000000000000224 RDX: ffff8afb9ee37c00 RSI: ffff8afb8da1a578 RDI: ffff8afb87e81280 RBP: ffff8afb83d67000 R08: 0000000000000001 R09: ffff8afb9652f850 R10: ffff960cc2df7908 R11: 0000000000000002 R12: 0000000000000000 R13: ffff8afb8d7688a0 R14: ffff8afb8da1a578 R15: 0000000000000224 FS: 00007f4dac35ce00(0000) GS:ffff8afe30b00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 000000010ddc6000 CR4: 00000000003506e0 Call Trace: <TASK> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? plist_add+0xbe/0x100 ? exc_page_fault+0x7c/0x180 ? asm_exc_page_fault+0x26/0x30 ? drm_dp_atomic_find_time_slots+0x5e/0x260 [drm_display_helper 0e67723696438d8e02b741593dd50d80b44c2026] ? drm_dp_atomic_find_time_slots+0x28/0x260 [drm_display_helper 0e67723696438d8e02b741593dd50d80b44c2026] compute_mst_dsc_configs_for_link+0x2ff/0xa40 [amdgpu 62e600d2a75e9158e1cd0a243bdc8e6da040c054] ? fill_plane_buffer_attributes+0x419/0x510 [amdgpu 62e600d2a75e9158e1cd0a243bdc8e6da040c054] compute_mst_dsc_configs_for_state+0x1e1/0x250 [amdgpu 62e600d2a75e9158e1cd0a243bdc8e6da040c054] amdgpu_dm_atomic_check+0xecd/0x1190 [amdgpu 62e600d2a75e9158e1cd0a243bdc8e6da040c054] drm_atomic_check_only+0x5c5/0xa40 drm_mode_atomic_ioctl+0x76e/0xbc0 [how] dsc recompute should be skipped if no mode change detected on the new request. If detected, keep checking whether the stream is already on current state or not. (cherry picked from commit 8151a6c13111b465dbabe07c19f572f7cbd16fef)	5.5	More Details
CVE-2024-43907	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules Check the pointer value to fix potential null pointer dereference	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43897	In the Linux kernel, the following vulnerability has been resolved: net: drop bad gso csum_start and offset in virtio_net_hdr Tighten csum_start and csum_offset checks in virtio_net_hdr_to_skb for GSO packets. The function already checks that a checksum requested with VIRTIO_NET_HDR_F_NEEDS_CSUM is in skb linear. But for GSO packets this might not hold for segs after segmentation. Syzkaller demonstrated to reach this warning in skb_checksum_help offset = skb_checksum_start_offset(skb); ret = -EINVAL; if (WARN_ON_ONCE(offset >= skb_headlen(skb))) By injecting a TSO packet: WARNING: CPU: 1 PID: 3539 at net/core/dev.c:3284 skb_checksum_help+0x3d0/0x5b0 ip_do_fragment+0x209/0x1b20 net/ipv4/ip_output.c:774 ip_finish_output_gso net/ipv4/ip_output.c:279 [inline] __ip_finish_output+0x2bd/0x4b0 net/ipv4/ip_output.c:301 iptunnel_xmit+0x50c/0x930 net/ipv4/ip_tunnel_core.c:82 ip_tunnel_xmit+0x2296/0x2c70 net/ipv4/ip_tunnel.c:813 __gre_xmit net/ipv4/ip_gre.c:469 [inline] ipgre_xmit+0x759/0xa60 net/ipv4/ip_gre.c:661 __netdev_start_xmit include/linux/netdevice.h:4850 [inline] netdev_start_xmit include/linux/netdevice.h:4864 [inline] xmit_one net/core/dev.c:3595 [inline] dev_hard_start_xmit+0x261/0x8c0 net/core/dev.c:3611 __dev_queue_xmit+0x1b97/0x3c90 net/core/dev.c:4261 packet_snd net/packet/af_packet.c:3073 [inline] The geometry of the bad input packet at tcp_gso_segment: [52.003050][T8403] skb len=12202 headroom=244 headlen=12093 tailroom=0 [52.003050][T8403] mac=(168,24) mac_len=24 net=(192,52) trans=244 [52.003050][T8403] shinfo(txflags=0 nr_frags=1 gso(size=1552 type=3 segs=0)) [52.003050][T8403] csum(0x60000c7 start=199 offset=1536 ip_summed=3 complete_sw=0 valid=0 level=0) Mitigate with stricter input validation. csum_offset: for GSO packets, deduce the correct value from gso_type. This is already done for USO. Extend it to TSO. Let UFO be: udp[46]_ufo_fragment ignores these fields and always computes the checksum in software. csum_start: finding the real offset requires parsing to the transport header. Do not add a parser, use existing segmentation parsing. Thanks to SKB_GSO_DODGY, that also catches bad packets that are hw offloaded. Again test both TSO and USO. Do not test UFO for the above reason, and do not test UDP tunnel offload. GSO packet are almost always CHECKSUM_PARTIAL. USO packets may be CHECKSUM_NONE since commit 10154dbded6d6 ("udp: Allow GSO transmit from devices with no checksum offload"), but then still these fields are initialized correctly in udp4_hwcsum/udp6_hwcsum_outgoing. So no need to test for ip_summed == CHECKSUM_PARTIAL first. This revises an existing fix mentioned in the Fixes tag, which broke small packets with GSO offload, as detected by kselftests.	5.5	More Details
CVE-2024-43906	In the Linux kernel, the following vulnerability has been resolved: drm/admgpu: fix dereferencing null pointer context When user space sets an invalid ta type, the pointer context will be empty. So it need to check the pointer context before using it	5.5	More Details
CVE-2024-43899	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix null pointer deref in dcn20_resource.c Fixes a hang thats triggered when MPV is run on a DCN401 dGPU: mpv --hwdec=vaapi --vo=gpu --hwdec-codecs=all and then enabling fullscreen playback (double click on the video) The following calltrace will be seen: [181.843989] BUG: kernel NULL pointer dereference, address: 0000000000000000 [181.843997] #PF: supervisor instruction fetch in kernel mode [181.844003] #PF: error_code(0x0010) - not-present page [181.844009] PGD 0 P4D 0 [181.844020] Oops: 0010 [#1] PREEMPT SMP NOPTI [181.844028] CPU: 6 PID: 1892 Comm: gnome-shell Tainted: G W OE 6.5.0-41-generic #41~22.04.2-Ubuntu [181.844038] Hardware name: System manufacturer System Product Name/CROSSHAIR VI HERO, BIOS 6302 10/23/2018 [181.844044] RIP: 0010:0x0 [181.844079] Code: Unable to access opcode bytes at 0xffffffffffffffd6. [181.844084] RSP: 0018:ffffb593c2b8f7b0 EFLAGS: 00010246 [181.844093] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000004 [181.844099] RDX: ffffb593c2b8f804 RSI: ffffb593c2b8f7e0 RDI: ffff9e3c8e758400 [181.844105] RBP: ffffb593c2b8f7b8 R08: ffffb593c2b8f9c8 R09: ffffb593c2b8f96c [181.844110] R10: 0000000000000000 R11: 0000000000000000 R12: ffffb593c2b8f9c8 [181.844115] R13: 0000000000000001 R14: ffff9e3c88000000 R15: 0000000000000005 [181.844121] FS: 00007c6e323bb5c0(0000) GS:ffff9e3f85f80000(0000) knlGS:0000000000000000 [181.844128] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [181.844134] CR2: ffffffffffffffd6 CR3: 0000000140fbe000 CR4: 00000000003506e0 [181.844141] Call Trace: [181.844146] <TASK> [181.844153] ? show_regs+0x6d/0x80 [181.844167] ? __die+0x24/0x80 [181.844179] ? page_fault_oops+0x99/0x1b0 [181.844192] ? do_user_addr_fault+0x31d/0x6b0 [181.844204] ? exc_page_fault+0x83/0x1b0 [181.844216] ? asm_exc_page_fault+0x27/0x30 [181.844237] dcn20_get_dcc_compression_cap+0x23/0x30 [amdgpu] [181.845115] amdgpu_dm_plane_validate_dcc.constprop.0+0xe5/0x180 [amdgpu] [181.845985] amdgpu_dm_plane_fill_plane_buffer_attributes+0x300/0x580 [amdgpu] [181.846848] fill_dc_plane_info_and_addr+0x258/0x350 [amdgpu] [181.847734] fill_dc_plane_attributes+0x162/0x350 [amdgpu] [181.848748] dm_update_plane_state.constprop.0+0x4e3/0x6b0 [amdgpu] [181.849791] ? dm_update_plane_state.constprop.0+0x4e3/0x6b0 [amdgpu] [181.850840] amdgpu_dm_atomic_check+0xdfe/0x1760 [amdgpu]	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43889	In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are.	5.5	More Details
CVE-2023-52904	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix possible NULL pointer dereference in snd_usb_pcm_has_fixed_rate() The subs function argument may be NULL, so do not use it before the NULL check.	5.5	More Details
CVE-2024-43901	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL pointer dereference for DTN log in DCN401 When users run the command: cat /sys/kernel/debug/dri/0/amdgpu_dm_dtn_log The following NULL pointer dereference happens: [+0.000003] BUG: kernel NULL pointer dereference, address: NULL [+0.000005] #PF: supervisor instruction fetch in kernel mode [+0.000002] #PF: error_code(0x0010) - not-present page [+0.000002] PGD 0 P4D 0 [+0.000004] Oops: 0010 [#1] PREEMPT SMP NOPTI [+0.000003] RIP: 0010:0x0 [+0.000008] Code: Unable to access opcode bytes at 0xffffffffffffffd6. [...] [+0.000002] PKRU: 55555554 [+0.000002] Call Trace: [+0.000002] <TASK> [+0.000003] ? show_regs+0x65/0x70 [+0.000006] ? __die+0x24/0x70 [+0.000004] ? page_fault_oops+0x160/0x470 [+0.000006] ? do_user_addr_fault+0x2b5/0x690 [+0.000003] ? prb_read_valid+0x1c/0x30 [+0.000005] ? exc_page_fault+0x8c/0x1a0 [+0.000005] ? asm_exc_page_fault+0x27/0x30 [+0.000012] dcn10_log_color_state+0xf9/0x510 [amdgpu] [+0.000306] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000003] ? vsnprintf+0x2fb/0x600 [+0.000009] dcn10_log_hw_state+0xfd0/0xfe0 [amdgpu] [+0.000218] ? __mod_memcg_lruvec_state+0xe8/0x170 [+0.000008] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? debug_smp_processor_id+0x17/0x20 [+0.000003] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? set_ptes.isra.0+0x2b/0x90 [+0.000004] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? _raw_spin_unlock+0x19/0x40 [+0.000004] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? do_anonymous_page+0x337/0x700 [+0.000004] dtn_log_read+0x82/0x120 [amdgpu] [+0.000207] full_proxy_read+0x66/0x90 [+0.000007] vfs_read+0xb0/0x340 [+0.000005] ? __count_memcg_events+0x79/0xe0 [+0.000002] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000003] ? count_memcg_events.constprop.0+0x1e/0x40 [+0.000003] ? handle_mm_fault+0xb2/0x370 [+0.000003] ksys_read+0x6b/0xf0 [+0.000004] __x64_sys_read+0x19/0x20 [+0.000003] do_syscall_64+0x60/0x130 [+0.000004] entry_SYSCALL_64_after_hwframe+0x6e/0x76 [+0.000003] RIP: 0033:0x7fdf32f147e2 [...] This error happens when the color log tries to read the gamut remap information from DCN401 which is not initialized in the dcn401_dpp_funcs which leads to a null pointer dereference. This commit addresses this issue by adding a proper guard to access the gamut_remap callback in case the specific ASIC did not implement this function.	5.5	More Details
CVE-2024-43902	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checker before passing variables Checks null pointer before passing variables to functions. This fixes 3 NULL_RETURNS issues reported by Coverity.	5.5	More Details
CVE-2024-43904	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checks for 'stream' and 'plane' before dereferencing This commit adds null checks for the 'stream' and 'plane' variables in the dcn30_apply_idle_power_optimizations function. These variables were previously assumed to be null at line 922, but they were used later in the code without checking if they were null. This could potentially lead to a null pointer dereference, which would cause a crash. The null checks ensure that 'stream' and 'plane' are not null before they are used, preventing potential crashes. Fixes the below static smatch checker: drivers/gpu/drm/amd/amdgpu/../display/dc/hwss/dcn30/dcn30_hwseq.c:938 dcn30_apply_idle_power_optimizations() error: we previously assumed 'stream' could be null (see line 922) drivers/gpu/drm/amd/amdgpu/../display/dc/hwss/dcn30/dcn30_hwseq.c:940 dcn30_apply_idle_power_optimizations() error: we previously assumed 'plane' could be null (see line 922)	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48889	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: sof-nau8825: fix module alias overflow The maximum name length for a platform_device_id entry is 20 characters including the trailing NUL byte. The sof_nau8825.c file exceeds that, which causes an obscure error message: sound/soc/intel/boards/snd-soc-sof_nau8825.mod.c:35:45: error: illegal character encoding in string literal [-Werror,-Winvalid-source-encoding] MODULE_ALIAS("platform:adl_max98373_nau8825<U+0018><AA>"); ^~~~ include/linux/module.h:168:49: note: expanded from macro 'MODULE_ALIAS' ^~~~~~ include/linux/module.h:165:56: note: expanded from macro 'MODULE_INFO' ^~~~ include/linux/moduleparam.h:26:47: note: expanded from macro '__MODULE_INFO' = __MODULE_INFO_PREFIX __stringify(tag) "=" info I could not figure out how to make the module handling robust enough to handle this better, but as a quick fix, using slightly shorter names that are still unique avoids the build issue.	5.5	More Details
CVE-2023-52907	In the Linux kernel, the following vulnerability has been resolved: nfc: pn533: Wait for out_urb's completion in pn533_usb_send_frame() Fix a use-after-free that occurs in hcd when in_urb sent from pn533_usb_send_frame() is completed earlier than out_urb. Its callback frees the skb data in pn533_send_async_complete() that is used as a transfer buffer of out_urb. Wait before sending in_urb until the callback of out_urb is called. To modify the callback of out_urb alone, separate the complete function of out_urb and ack_urb. Found by a modified version of syzkaller. BUG: KASAN: use-after-free in dummy_timer Call Trace: memcpy (mm/kasan/shadow.c:65) dummy_perform_transfer (drivers/usb/gadget/udc/dummy_hcd.c:1352) transfer (drivers/usb/gadget/udc/dummy_hcd.c:1453) dummy_timer (drivers/usb/gadget/udc/dummy_hcd.c:1972) arch_static_branch (arch/x86/include/asm/jump_label.h:27) static_key_false (include/linux/jump_label.h:207) timer_expire_exit (include/trace/events/timer.h:127) call_timer_fn (kernel/time/timer.c:1475) expire_timers (kernel/time/timer.c:1519) __run_timers (kernel/time/timer.c:1790) run_timer_softirq (kernel/time/timer.c:1803)	5.5	More Details
CVE-2024-43886	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null check in resource_log_pipe_topology_update [WHY] When switching from "Extend" to "Second Display Only" we sometimes call resource_get_otg_master_for_stream on a stream for the eDP, which is disconnected. This leads to a null pointer dereference. [HOW] Added a null check in dc_resource.c/resource_log_pipe_topology_update.	5.5	More Details
CVE-2023-52912	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fixed bug on error when unloading amdgpu Fixed bug on error when unloading amdgpu. The error message is as follows: [377.706202] kernel BUG at drivers/gpu/drm/drm_buddy.c:278! [377.706215] invalid opcode: 0000 [#1] PREEMPT SMP NOPTI [377.706222] CPU: 4 PID: 8610 Comm: modprobe Tainted: G IOE 6.0.0-thomas #1 [377.706231] Hardware name: ASUS System Product Name/PRIME Z390-A, BIOS 2004 11/02/2021 [377.706238] RIP: 0010:drm_buddy_free_block+0x26/0x30 [drm_buddy] [377.706264] Code: 00 00 00 90 0f 1f 44 00 00 48 8b 0e 89 c8 25 00 0c 00 00 3d 00 04 00 00 75 10 48 8b 47 18 48 d3 e0 48 01 47 28 e9 fa fe ff ff <0f> 0b 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 41 54 55 48 89 f5 53 [377.706282] RSP: 0018:ffffad2dc4683cb8 EFLAGS: 00010287 [377.706289] RAX: 0000000000000000 RBX: ffff8b1743bd5138 RCX: 0000000000000000 [377.706297] RDX: ffff8b1743bd5160 RSI: ffff8b1743bd5c78 RDI: ffff8b16d1b25f70 [377.706304] RBP: ffff8b1743bd59e0 R08: 0000000000000001 R09: 0000000000000001 [377.706311] R10: ffff8b16c8572400 R11: ffffad2dc4683cf0 R12: ffff8b16d1b25f70 [377.706318] R13: ffff8b16d1b25fd0 R14: ffff8b1743bd59c0 R15: ffff8b16d1b25f70 [377.706325] FS: 00007fec56c72c40(0000) GS:ffff8b1836500000(0000) knlGS:0000000000000000 [377.706334] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [377.706340] CR2: 00007f9b88c1ba50 CR3: 0000000110450004 CR4: 00000000003706e0 [377.706347] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [377.706354] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [377.706361] Call Trace: [377.706365] <TASK> [377.706369] drm_buddy_free_list+0x2a/0x60 [drm_buddy] [377.706376] amdgpu_vram_mgr_fini+0xea/0x180 [amdgpu] [377.706572] amdgpu_ttm_fini+0x12e/0x1a0 [amdgpu] [377.706650] amdgpu_bo_fini+0x22/0x90 [amdgpu] [377.706727] gmc_v11_0_sw_fini+0x26/0x30 [amdgpu] [377.706821] amdgpu_device_fini_sw+0xa1/0x3c0 [amdgpu] [377.706897] amdgpu_driver_release_kms+0x12/0x30 [amdgpu] [377.706975] drm_dev_release+0x20/0x40 [drm] [377.707006] release_nodes+0x35/0xb0 [377.707014] devres_release_all+0x8b/0xc0 [377.707020] device_unbind_cleanup+0xe/0x70 [377.707027] device_release_driver_internal+0xee/0x160 [377.707033] driver_detach+0x44/0x90 [377.707039] bus_remove_driver+0x55/0xe0 [377.707045] pci_unregister_driver+0x3b/0x90 [377.707052] amdgpu_exit+0x11/0x6c [amdgpu] [377.707194] __x64_sys_delete_module+0x142/0x2b0 [377.707201] ? fpregs_assert_state_consistent+0x22/0x50 [377.707208] ? exit_to_user_mode_prepare+0x3e/0x190 [377.707215] do_syscall_64+0x38/0x90 [377.707221] entry_SYSCALL_64_after_hwframe+0x63/0xcd	5.5	More Details
CVE-2024-43871	In the Linux kernel, the following vulnerability has been resolved: devres: Fix memory leakage caused by driver API devm_free_percpu() It will cause memory leakage when use driver API devm_free_percpu() to free memory allocated by devm_alloc_percpu(), fixed by using devres_release() instead of devres_destroy() within devm_free_percpu().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43872	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix soft lockup under heavy CEQE load CEQEs are handled in interrupt handler currently. This may cause the CPU core staying in interrupt context too long and lead to soft lockup under heavy load. Handle CEQEs in BH workqueue and set an upper limit for the number of CEQE handled by a single call of work handler.	5.5	More Details
CVE-2024-43874	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Fix null pointer dereference in __sev_snp_shutdown_locked Fix a null pointer dereference induced by DEBUG_TEST_DRIVER_REMOVE. Return from __sev_snp_shutdown_locked() if the psp_device or the sev_device structs are not initialized. Without the fix, the driver will produce the following splat: ccp 0000:55:00.5: enabling device (0000 -> 0002) ccp 0000:55:00.5: sev enabled ccp 0000:55:00.5: psp enabled BUG: kernel NULL pointer dereference, address: 00000000000000f0 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP DEBUG_PAGEALLOC NOPTI CPU: 262 PID: 1 Comm: swapper/0 Not tainted 6.9.0-rc1+ #29 RIP: 0010:__sev_snp_shutdown_locked+0x2e/0x150 Code: 00 55 48 89 e5 41 57 41 56 41 54 53 48 83 ec 10 41 89 f7 49 89 fe 65 48 8b 04 25 28 00 00 00 48 89 45 d8 48 8b 05 6a 5a 7f 06 <4c> 8b a0 f0 00 00 00 41 0f b6 9c 24 a2 00 00 00 48 83 fb 02 0f 83 RSP: 0018:ffffb2ea4014b7b8 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffff9e4acd2e0a28 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffffb2ea4014b808 RBP: ffffb2ea4014b7e8 R08: 0000000000000106 R09: 000000000003d9c0 R10: 0000000000000001 R11: ffffffffa39ff070 R12: ffff9e49d40590c8 R13: 0000000000000000 R14: ffffb2ea4014b808 R15: 0000000000000000 FS: 0000000000000000(0000) GS:ffff9e58b1e00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000000000f0 CR3: 0000000418a3e001 CR4: 0000000000770ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body+0x6f/0xb0 ? __die+0xcc/0xf0 ? page_fault_oops+0x330/0x3a0 ? save_trace+0x2a5/0x360 ? do_user_addr_fault+0x583/0x630 ? exc_page_fault+0x81/0x120 ? asm_exc_page_fault+0x2b/0x30 ? __sev_snp_shutdown_locked+0x2e/0x150 __sev_firmware_shutdown+0x349/0x5b0 ? pm_runtime_barrier+0x66/0xe0 sev_dev_destroy+0x34/0xb0 psp_dev_destroy+0x27/0x60 sp_destroy+0x39/0x90 sp_pci_remove+0x22/0x60 pci_device_remove+0x4e/0x110 really_probe+0x271/0x4e0 __driver_probe_device+0x8f/0x160 driver_probe_device+0x24/0x120 __driver_attach+0xc7/0x280 ? driver_attach+0x30/0x30 bus_for_each_dev+0x10d/0x130 driver_attach+0x22/0x30 bus_add_driver+0x171/0x2b0 ? unaccepted_memory_init_kdump+0x20/0x20 driver_register+0x67/0x100 __pci_register_driver+0x83/0x90 sp_pci_init+0x22/0x30 sp_mod_init+0x13/0x30 do_one_initcall+0xb8/0x290 ? sched_clock_noinstr+0xd/0x10 ? local_clock_noinstr+0x3e/0x100 ? stack_depot_save_flags+0x21e/0x6a0 ? local_clock+0x1c/0x60 ? stack_depot_save_flags+0x21e/0x6a0 ? sched_clock_noinstr+0xd/0x10 ? local_clock_noinstr+0x3e/0x100 ? __lock_acquire+0xd90/0xe30 ? sched_clock_noinstr+0xd/0x10 ? local_clock_noinstr+0x3e/0x100 ? __create_object+0x66/0x100 ? local_clock+0x1c/0x60 ? __create_object+0x66/0x100 ? parameq+0x1b/0x90 ? parse_one+0x6d/0x1d0 ? parse_args+0xd7/0x1f0 ? do_initcall_level+0x180/0x180 do_initcall_level+0xb0/0x180 do_initcalls+0x60/0xa0 ? kernel_init+0x1f/0x1d0 do_basic_setup+0x41/0x50 kernel_init_freeable+0x1ac/0x230 ? rest_init+0x1f0/0x1f0 kernel_init+0x1f/0x1d0 ? rest_init+0x1f0/0x1f0 ret_from_fork+0x3d/0x50 ? rest_init+0x1f0/0x1f0 ret_from_fork_asm+0x11/0x20 </TASK> Modules linked in: CR2: 00000000000000f0 ---[end trace 0000000000000000]--- RIP: 0010:__sev_snp_shutdown_locked+0x2e/0x150 Code: 00 55 48 89 e5 41 57 41 56 41 54 53 48 83 ec 10 41 89 f7 49 89 fe 65 48 8b 04 25 28 00 00 00 48 89 45 d8 48 8b 05 6a 5a 7f 06 <4c> 8b a0 f0 00 00 00 41 0f b6 9c 24 a2 00 00 00 48 83 fb 02 0f 83 RSP: 0018:ffffb2ea4014b7b8 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffff9e4acd2e0a28 RCX: 0000000000000000 RDX: 0000000 ---truncated---	5.5	More Details
CVE-2024-6767	The WordSurvey plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘sounding_title’ parameter in all versions up to, and including, 3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, 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-2023-52914	In the Linux kernel, the following vulnerability has been resolved: io_uring/poll: add hash if ready poll request can't complete inline If we don't, then we may lose access to it completely, leading to a request leak. This will eventually stall the ring exit process as well.	5.5	More Details
CVE-2023-52913	In the Linux kernel, the following vulnerability has been resolved: drm/i915: Fix potential context UAFs gem_context_register() makes the context visible to userspace, and which point a separate thread can trigger the I915_GEM_CONTEXT_DESTROY ioctl. So we need to ensure that nothing uses the ctx ptr after this. And we need to ensure that adding the ctx to the xarray is the *last* thing that gem_context_register() does with the ctx pointer. [tursulin: Stable and fixes tags add/tidy.] (cherry picked from commit bed4b455cf5374e68879be56971c1da563bcd90c)	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52911	In the Linux kernel, the following vulnerability has been resolved: drm/msm: another fix for the headless Adreno GPU Fix another oops reproducible when rebooting the board with the Adreno GPU working in the headless mode (e.g. iMX platforms). Unable to handle kernel NULL pointer dereference at virtual address 00000000 when read [00000000] *pgd=74936831, *pte=00000000, *ppte=00000000 Internal error: Oops: 17 [#1] ARM CPU: 0 PID: 51 Comm: reboot Not tainted 6.2.0-rc1-dirty #11 Hardware name: Freescale i.MX53 (Device Tree Support) PC is at msm_atomic_commit_tail+0x50/0x970 LR is at commit_tail+0x9c/0x188 pc : [<c06aa430>] lr : [<c067a214>] psr: 600e0013 sp : e0851d30 ip : ee4eb7eb fp : 00090acc r10: 00000058 r9 : c2193014 r8 : c4310000 r7 : c4759380 r6 : 07bef61d r5 : 00000000 r4 : 00000000 r3 : c44cc440 r2 : 00000000 r1 : 00000000 r0 : 00000000 Flags: nZCv IRQs on FIQs on Mode SVC_32 ISA ARM Segment none Control: 10c5387d Table: 74910019 DAC: 00000051 Register r0 information: NULL pointer Register r1 information: NULL pointer Register r2 information: NULL pointer Register r3 information: slab kmalloc-1k start c44cc400 pointer offset 64 size 1024 Register r4 information: NULL pointer Register r5 information: NULL pointer Register r6 information: non-paged memory Register r7 information: slab kmalloc-128 start c4759380 pointer offset 0 size 128 Register r8 information: slab kmalloc-2k start c4310000 pointer offset 0 size 2048 Register r9 information: non-slab/vmalloc memory Register r10 information: non-paged memory Register r11 information: non-paged memory Register r12 information: non-paged memory Process reboot (pid: 51, stack limit = 0xc80046d9) Stack: (0xe0851d30 to 0xe0852000) 1d20: c4759380 fbd77200 000005ff 002b9c70 1d40: c4759380 c4759380 00000000 07bef61d 00000600 c0d6fe7c c2193014 00000058 1d60: 00090acc c067a214 00000000 c4759380 c4310000 00000000 c44cc854 c067a89c 1d80: 00000000 00000000 00000000 c4310468 00000000 c4759380 c4310000 c4310468 1da0: c4310470 c0643258 c4759380 00000000 00000000 c0c4ee24 00000000 c44cc810 1dc0: 00000000 c0c4ee24 00000000 c44cc810 00000000 0347d2a8 e0851e00 e0851e00 1de0: c4759380 c067ad20 c4310000 00000000 c44cc810 c27f8718 c44cc854 c067adb8 1e00: c4933000 00000002 00000001 00000000 00000000 c2130850 00000000 c2130854 1e20: c25fc488 00000000 c0ff162c 00000000 00000001 00000002 00000000 00000000 1e40: c43102c0 c43102c0 00000000 0347d2a8 c44cc810 c44cc814 c2133da8 c06d1a60 1e60: 00000000 00000000 00079028 c2012f24 fee1dead c4933000 00000058 c01431e4 1e80: 01234567 c0143a20 00000000 00000000 00000000 00000000 00000000 00000000 1ea0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1ec0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1ee0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1f00: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1f20: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1f40: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1f60: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 1f80: 00000000 00000000 00000000 0347d2a8 00000002 00000004 00000078 00000058 1fa0: c010028c c0100060 00000002 00000004 fee1dead 28121969 01234567 00079028 1fc0: 00000002 00000004 00000078 00000058 0002fdc5 00000000 00000000 00090acc 1fe0: 00000058 becc9c64 b6e97e05 b6e0e5f6 600e0030 fee1dead 00000000 00000000 msm_atomic_commit_tail from commit_tail+0x9c/0x188 commit_tail from drm_atomic_helper_commit+0x160/0x188 drm_atomic_helper_commit from drm_atomic_commit+0xac/0xe0 drm_atomic_commit from drm_atomic_helper_disable_all+0x1b0/0x1c0 drm_atomic_helper_disable_all from drm_atomic_helper_shutdown+0x88/0x140 drm_atomic_helper_shutdown from device_shutdown+0x16c/0x240 device_shutdown from kernel_restart+0x38/0x90 kernel_restart from __do_sys_reboot+0x ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43910	In the Linux kernel, the following vulnerability has been resolved: bpf: add missing check_func_arg_reg_off() to prevent out-of-bounds memory accesses Currently, it's possible to pass in a modified CONST_PTR_TO_DYNPTR to a global function as an argument. The adverse effects of this is that BPF helpers can continue to make use of this modified CONST_PTR_TO_DYNPTR from within the context of the global function, which can unintentionally result in out-of-bounds memory accesses and therefore compromise overall system stability i.e. [244.157771] BUG: KASAN: slab-out-of-bounds in bpf_dynptr_data+0x137/0x140 [244.161345] Read of size 8 at addr ffff88810914be68 by task test_progs/302 [244.167151] CPU: 0 PID: 302 Comm: test_progs Tainted: G O E 6.10.0-rc3-00131-g66b586715063 #533 [244.174318] Call Trace: [244.175787] <TASK> [244.177356] dump_stack_lvl+0x66/0xa0 [244.179531] print_report+0xce/0x670 [244.182314] ? __virt_addr_valid+0x200/0x3e0 [244.184908] kasan_report+0xd7/0x110 [244.187408] ? bpf_dynptr_data+0x137/0x140 [244.189714] ? bpf_dynptr_data+0x137/0x140 [244.192020] bpf_dynptr_data+0x137/0x140 [244.194264] bpf_prog_b02a02fdd2bdc5fa_global_call_bpf_dynptr_data+0x22/0x26 [244.198044] bpf_prog_b0fe7b9d7dc3abde_callback_adjust_bpf_dynptr_reg_off+0x1f/0x23 [244.202136] bpf_user_ringbuf_drain+0x2c7/0x570 [244.204744] ? 0xffffffffc0009e58 [244.206593] ? __pfx_bpf_user_ringbuf_drain+0x10/0x10 [244.209795] bpf_prog_33ab33f6a804ba2d_user_ringbuf_callback_const_ptr_to_dynptr_reg_off+0x47/0x4b [244.215922] bpf_trampoline_6442502480+0x43/0xe3 [244.218691] __x64_sys_prlimit64+0x9/0xf0 [244.220912] do_syscall_64+0xc1/0x1d0 [244.223043] entry_SYSCALL_64_after_hwframe+0x77/0x7f [244.226458] RIP: 0033:0x7ffa3eb8f059 [244.228582] Code: 08 89 e8 5b 5d c3 66 2e 0f 1f 84 00 00 00 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 8b 0d 8f 1d 0d 00 f7 d8 64 89 01 48 [244.241307] RSP: 002b:00007ffa3e9c6eb8 EFLAGS: 00000206 ORIG_RAX: 000000000000012e [244.246474] RAX: ffffffffffffffda RBX: 00007ffa3e9c7cdc RCX: 00007ffa3eb8f059 [244.250478] RDX: 00007ffa3eb162b4 RSI: 0000000000000000 RDI: 00007ffa3e9c7fb0 [244.255396] RBP: 00007ffa3e9c6ed0 R08: 00007ffa3e9c76c0 R09: 0000000000000000 [244.260195] R10: 0000000000000000 R11: 0000000000000206 R12: ffffffffffffff80 [244.264201] R13: 000000000000001c R14: 00007ffc5d6b4260 R15: 00007ffa3e1c7000 [244.268303] </TASK> Add a check_func_arg_reg_off() to the path in which the BPF verifier verifies the arguments of global function arguments, specifically those which take an argument of type ARG_PTR_TO_DYNPTR | MEM_RDONLY. Also, process_dynptr_func() doesn't appear to perform any explicit and strict type matching on the supplied register type, so let's also enforce that a register either type PTR_TO_STACK or CONST_PTR_TO_DYNPTR is by the caller.	5.5	More Details
CVE-2024-8011	Logitech Options+ on MacOS prior 1.72 allows a local attacker to inject dynamic library within Options+ runtime and abuse permissions granted by the user to Options+ such as Camera.	5.5	More Details
CVE-2023-52910	In the Linux kernel, the following vulnerability has been resolved: iommu/iova: Fix alloc iova overflows issue In __alloc_and_insert_iova_range, there is an issue that retry_pfn overflows. The value of iovad->anchor.pfn_hi is ~0UL, then when iovad->cached_node is iovad->anchor, curr_iova->pfn_hi + 1 will overflow. As a result, if the retry logic is executed, low_pfn is updated to 0, and then new_pfn < low_pfn returns false to make the allocation successful. This issue occurs in the following two situations: 1. The first iova size exceeds the domain size. When initializing iova domain, iovad->cached_node is assigned as iovad->anchor. For example, the iova domain size is 10M, start_pfn is 0x1_F000_0000, and the iova size allocated for the first time is 11M. The following is the log information, new->pfn_lo is smaller than iovad->cached_node. Example log as follows: [223.798112][T1705487] sh: [name:iova&]__alloc_and_insert_iova_range start_pfn:0x1f0000,retry_pfn:0x0,size:0xb00,limit_pfn:0x1f0a00 [223.799590][T1705487] sh: [name:iova&]__alloc_and_insert_iova_range success start_pfn:0x1f0000,new->pfn_lo:0x1efe00,new->pfn_hi:0x1f08ff 2. The node with the largest iova->pfn_lo value in the iova domain is deleted, iovad->cached_node will be updated to iovad->anchor, and then the alloc iova size exceeds the maximum iova size that can be allocated in the domain. After judging that retry_pfn is less than limit_pfn, call retry_pfn+1 to fix the overflow issue.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48868	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: Let probe fail when workqueue cannot be enabled The workqueue is enabled when the appropriate driver is loaded and disabled when the driver is removed. When the driver is removed it assumes that the workqueue was enabled successfully and proceeds to free allocations made during workqueue enabling. Failure during workqueue enabling does not prevent the driver from being loaded. This is because the error path within drv_enable_wq() returns success unless a second failure is encountered during the error path. By returning success it is possible to load the driver even if the workqueue cannot be enabled and allocations that do not exist are attempted to be freed during driver remove. Some examples of problematic flows: (a) idxd_dmaengine_drv_probe() -> drv_enable_wq() -> idxd_wq_request_irq(): In above flow, if idxd_wq_request_irq() fails then idxd_wq_unmap_portal() is called on error exit path, but drv_enable_wq() returns 0 because idxd_wq_disable() succeeds. The driver is thus loaded successfully. idxd_dmaengine_drv_remove()->drv_disable_wq()->idxd_wq_unmap_portal() Above flow on driver unload triggers the WARN in devm_iounmap() because the device resource has already been removed during error path of drv_enable_wq(). (b) idxd_dmaengine_drv_probe() -> drv_enable_wq() -> idxd_wq_request_irq(): In above flow, if idxd_wq_request_irq() fails then idxd_wq_init_percpu_ref() is never called to initialize the percpu counter, yet the driver loads successfully because drv_enable_wq() returns 0. idxd_dmaengine_drv_remove()->__idxd_wq_quiesce()->percpu_ref_kill(): Above flow on driver unload triggers a BUG when attempting to drop the initial ref of the uninitialized percpu ref: BUG: kernel NULL pointer dereference, address: 0000000000000010 Fix the drv_enable_wq() error path by returning the original error that indicates failure of workqueue enabling. This ensures that the probe fails when an error is encountered and the driver remove paths are only attempted when the workqueue was enabled successfully.	5.5	More Details
CVE-2023-52908	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix potential NULL dereference Fix potential NULL dereference, in the case when "man", the resource manager might be NULL, when/if we print debug information.	5.5	More Details
CVE-2022-48870	In the Linux kernel, the following vulnerability has been resolved: tty: fix possible null-ptr-defer in spk_ttyio_release Run the following tests on the qemu platform: syzkaller:~# modprobe speakup_audptr input: Speakup as /devices/virtual/input/input4 initialized device: /dev/synth, node (MAJOR 10, MINOR 125) speakup 3.1.6: initialized synth name on entry is: (null) synth probe spk_ttyio_initialise_ldisc failed because tty_kopen_exclusive returned failed (errno -16), then remove the module, we will get a null-ptr-defer problem, as follow: syzkaller:~# modprobe -r speakup_audptr releasing synth audptr BUG: kernel NULL pointer dereference, address: 0000000000000080 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] PREEMPT SMP PTI CPU: 2 PID: 204 Comm: modprobe Not tainted 6.1.0-rc6-dirty #1 RIP: 0010:mutex_lock+0x14/0x30 Call Trace: <TASK> spk_ttyio_release+0x19/0x70 [speakup] synth_release.part.6+0xac/0xc0 [speakup] synth_remove+0x56/0x60 [speakup] __x64_sys_delete_module+0x156/0x250 ? fpregs_assert_state_consistent+0x1d/0x50 do_syscall_64+0x37/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd </TASK> Modules linked in: speakup_audptr(-) speakup Dumping ftrace buffer: in_synth->dev was not initialized during modprobe, so we add check for in_synth->dev to fix this bug.	5.5	More Details
CVE-2024-43884	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Add error handling to pair_device() hci_conn_params_add() never checks for a NULL value and could lead to a NULL pointer dereference causing a crash. Fixed by adding error handling in the function.	5.5	More Details
CVE-2024-43909	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference for smu7 optimize the code to avoid pass a null pointer (hwmgr->backend) to function smu7_update_edc_leakage_table.	5.5	More Details
CVE-2024-43912	In the Linux kernel, the following vulnerability has been resolved: wifi: nl80211: disallow setting special AP channel widths Setting the AP channel width is meant for use with the normal 20/40/... MHz channel width progression, and switching around in S1G or narrow channels isn't supported. Disallow that.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43911	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix NULL dereference at band check in starting tx ba session In MLD connection, link_data/link_conf are dynamically allocated. They don't point to vif->bss_conf. So, there will be no chanreq assigned to vif->bss_conf and then the chan will be NULL. Tweak the code to check ht_supported/vht_supported/has_he/has_eht on sta deflink. Crash log (with rtw89 version under MLO development): [9890.526087] BUG: kernel NULL pointer dereference, address: 0000000000000000 [9890.526102] #PF: supervisor read access in kernel mode [9890.526105] #PF: error_code(0x0000) - not-present page [9890.526109] PGD 0 P4D 0 [9890.526114] Oops: 0000 [#1] PREEMPT SMP PTI [9890.526119] CPU: 2 PID: 6367 Comm: kworker/u16:2 Kdump: loaded Tainted: G OE 6.9.0 #1 [9890.526123] Hardware name: LENOVO 2356AD1/2356AD1, BIOS G7ETB3WW (2.73) 11/28/2018 [9890.526126] Workqueue: phy2 rtw89_core_ba_work [rtw89_core] [9890.526203] RIP: 0010:ieee80211_start_tx_ba_session (net/mac80211/agg-tx.c:618 (discriminator 1)) mac80211 [9890.526279] Code: f7 e8 d5 93 3e ea 48 83 c4 28 89 d8 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc 49 8b 84 24 e0 f1 ff ff 48 8b 80 90 1b 00 00 <83> 38 03 0f 84 37 fe ff ff bb ea ff ff ff eb cc 49 8b 84 24 10 f3 All code ======== 0: f7 e8 imul %eax 2: d5 (bad) 3: 93 xchg %eax,%ebx 4: 3e ea ds (bad) 6: 48 83 c4 28 add $0x28,%rsp a: 89 d8 mov %ebx,%eax c: 5b pop %rbx d: 41 5c pop %r12 f: 41 5d pop %r13 11: 41 5e pop %r14 13: 41 5f pop %r15 15: 5d pop %rbp 16: c3 retq 17: cc int3 18: cc int3 19: cc int3 1a: cc int3 1b: 49 8b 84 24 e0 f1 ff mov -0xe20(%r12),%rax 22: ff 23: 48 8b 80 90 1b 00 00 mov 0x1b90(%rax),%rax 2a:* 83 38 03 cmpl $0x3,(%rax) <-- trapping instruction 2d: 0f 84 37 fe ff ff je 0xffffffffffffe6a 33: bb ea ff ff ff mov $0xffffffea,%ebx 38: eb cc jmp 0x6 3a: 49 rex.WB 3b: 8b .byte 0x8b 3c: 84 24 10 test %ah,(%rax,%rdx,1) 3f: f3 repz Code starting with the faulting instruction ========== 0: 83 38 03 cmpl $0x3,(%rax) 3: 0f 84 37 fe ff ff je 0xffffffffffffe40 9: bb ea ff ff ff mov $0xffffffea,%ebx e: eb cc jmp 0xffffffffffffffdc 10: 49 rex.WB 11: 8b .byte 0x8b 12: 84 24 10 test %ah,(%rax,%rdx,1) 15: f3 repz [9890.526285] RSP: 0018:ffffb8db09013d68 EFLAGS: 00010246 [9890.526291] RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff9308e0d656c8 [9890.526295] RDX: 0000000000000000 RSI: ffffffffab99460b RDI: ffffffffab9a7685 [9890.526300] RBP: ffffb8db09013db8 R08: 0000000000000000 R09: 0000000000000873 [9890.526304] R10: ffff9308e0d64800 R11: 0000000000000002 R12: ffff9308e5ff6e70 [9890.526308] R13: ffff930952500e20 R14: ffff9309192a8c00 R15: 0000000000000000 [9890.526313] FS: 0000000000000000(0000) GS:ffff930b4e700000(0000) knlGS:0000000000000000 [9890.526316] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [9890.526318] CR2: 0000000000000000 CR3: 0000000391c58005 CR4: 0000000001706f0 [9890.526321] Call Trace: [9890.526324] <TASK> [9890.526327] ? show_regs (arch/x86/kernel/dumpstack.c:479) [9890.526335] ? __die (arch/x86/kernel/dumpstack.c:421 arch/x86/kernel/dumpstack.c:434) [9890.526340] ? page_fault_oops (arch/x86/mm/fault.c:713) [9890.526347] ? search_module_extables (kernel/module/main.c:3256 (discriminator --- truncated---	5.5	More Details
CVE-2023-52895	In the Linux kernel, the following vulnerability has been resolved: io_uring/poll: don't reissue in case of poll race on multishot request A previous commit fixed a poll race that can occur, but it's only applicable for multishot requests. For a multishot request, we can safely ignore a spurious wakeup, as we never leave the waitqueue to begin with. A blunt reissue of a multishot armed request can cause us to leak a buffer, if they are ring provided. While this seems like a bug in itself, it's not really defined behavior to reissue a multishot request directly. It's less efficient to do so as well, and not required to rearm anything like it is for singleshot poll requests.	5.5	More Details
CVE-2023-52893	In the Linux kernel, the following vulnerability has been resolved: gsmi: fix null-deref in gsmi_get_variable We can get EFI variables without fetching the attribute, so we must allow for that in gsmi. commit 859748255b43 ("efi: pstore: Omit efivars caching EFI varstore access layer") added a new get_variable call with attr=NULL, which triggers panic in gsmi.	5.5	More Details
CVE-2022-48877	In the Linux kernel, the following vulnerability has been resolved: f2fs: let's avoid panic if extent_tree is not created This patch avoids the below panic. pc : __lookup_extent_tree+0xd8/0x760 lr : f2fs_do_write_data_page+0x104/0x87c sp : ffffffc010cbb3c0 x29: ffffffc010cbb3e0 x28: 0000000000000000 x27: ffffff8803e7f020 x26: ffffff8803e7ed40 x25: ffffff8803e7f020 x24: ffffffc010cbb460 x23: ffffffc010cbb480 x22: 0000000000000000 x21: 0000000000000000 x20: ffffffff22e90900 x19: 0000000000000000 x18: ffffffc010c5d080 x17: 0000000000000000 x16: 0000000000000020 x15: ffffffdb1acdbb88 x14: ffffff888759e2b0 x13: 0000000000000000 x12: ffffff802da49000 x11: 000000000a001200 x10: ffffff8803e7ed40 x9 : ffffff8023195800 x8 : ffffff802da49078 x7 : 0000000000000001 x6 : 0000000000000000 x5 : 0000000000000006 x4 : ffffffc010cbba28 x3 : 0000000000000000 x2 : ffffffc010cbb480 x1 : 0000000000000000 x0 : ffffff8803e7ed40 Call trace: __lookup_extent_tree+0xd8/0x760 f2fs_do_write_data_page+0x104/0x87c f2fs_write_single_data_page+0x420/0xb60 f2fs_write_cache_pages+0x418/0xb1c __f2fs_write_data_pages+0x428/0x58c f2fs_write_data_pages+0x30/0x40 do_writepages+0x88/0x190 __writeback_single_inode+0x48/0x448 writeback_sb_inodes+0x468/0x9e8 __writeback_inodes_wb+0xb8/0x2a4 wb_writeback+0x33c/0x740 wb_do_writeback+0x2b4/0x400 wb_workfn+0xe4/0x34c process_one_work+0x24c/0x5bc worker_thread+0x3e8/0xa50 kthread+0x150/0x1b4	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48897	In the Linux kernel, the following vulnerability has been resolved: arm64/mm: fix incorrect file_map_count for invalid pmd The page table check trigger BUG_ON() unexpectedly when split hugepage: ----------[cut here]---------- kernel BUG at mm/page_table_check.c:119! Internal error: Oops - BUG: 00000000f2000800 [#1] SMP Dumping ftrace buffer: (ftrace buffer empty) Modules linked in: CPU: 7 PID: 210 Comm: transhuge-stres Not tainted 6.1.0-rc3+ #748 Hardware name: linux,dummy-virt (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : page_table_check_set.isra.0+0x398/0x468 lr : page_table_check_set.isra.0+0x1c0/0x468 [...] Call trace: page_table_check_set.isra.0+0x398/0x468 __page_table_check_pte_set+0x160/0x1c0 __split_huge_pmd_locked+0x900/0x1648 __split_huge_pmd+0x28c/0x3b8 unmap_page_range+0x428/0x858 unmap_single_vma+0xf4/0x1c8 zap_page_range+0x2b0/0x410 madvise_vma_behavior+0xc44/0xe78 do_madvise+0x280/0x698 __arm64_sys_madvise+0x90/0xe8 invoke_syscall.constprop.0+0xdc/0x1d8 do_el0_svc+0xf4/0x3f8 el0_svc+0x58/0x120 el0t_64_sync_handler+0xb8/0xc0 el0t_64_sync+0x19c/0x1a0 [...] On arm64, pmd_leaf() will return true even if the pmd is invalid due to pmd_present_invalid() check. So in pmdp_invalidate() the file_map_count will not only decrease once but also increase once. Then in set_pte_at(), the file_map_count increase again, and so trigger BUG_ON() unexpectedly. Add !pmd_present_invalid() check in pmd_user_accessible_page() to fix the problem.	5.5	More Details
CVE-2022-48879	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services are not supported or have been disabled, the runtime services workqueue will never have been allocated. Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to avoid dereferencing a NULL pointer.	5.5	More Details
CVE-2022-48896	In the Linux kernel, the following vulnerability has been resolved: ixgbe: fix pci device refcount leak As the comment of pci_get_domain_bus_and_slot() says, it returns a PCI device with refcount incremented, when finish using it, the caller must decrement the reference count by calling pci_dev_put(). In ixgbe_get_first_secondary_devfn() and ixgbe_x550em_a_has_mii(), pci_dev_put() is called to avoid leak.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48895	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu: Don't unregister on shutdown Michael Walle says he noticed the following stack trace while performing a shutdown with "reboot -f". He suggests he got "lucky" and just hit the correct spot for the reboot while there was a packet transmission in flight. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000098 CPU: 0 PID: 23 Comm: kworker/0:1 Not tainted 6.1.0-rc5-00088-gf3600ff8e322 #1930 Hardware name: Kontron KBox A-230-LS (DT) pc : iommu_get_dma_domain+0x14/0x20 lr : iommu_dma_map_page+0x9c/0x254 Call trace: iommu_get_dma_domain+0x14/0x20 dma_map_page_attrs+0x1ec/0x250 enetc_start_xmit+0x14c/0x10b0 enetc_xmit+0x60/0xdc dev_hard_start_xmit+0xb8/0x210 sch_direct_xmit+0x11c/0x420 __dev_queue_xmit+0x354/0xb20 ip6_finish_output2+0x280/0x5b0 __ip6_finish_output+0x15c/0x270 ip6_output+0x78/0x15c NF_HOOK.constprop.0+0x50/0xd0 mld_sendpack+0x1bc/0x320 mld_ifc_work+0x1d8/0x4dc process_one_work+0x1e8/0x460 worker_thread+0x178/0x534 kthread+0xe0/0xe4 ret_from_fork+0x10/0x20 Code: d503201f f9416800 d503233f d50323bf (f9404c00) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception in interrupt This appears to be reproducible when the board has a fixed IP address, is ping flooded from another host, and "reboot -f" is used. The following is one more manifestation of the issue: $ reboot -f kvm: exiting hardware virtualization cfg80211: failed to load regulatory.db arm-smmu 5000000.iommu: disabling translation sdhci-esdhc 2140000.mmc: Removing from iommu group 11 sdhci-esdhc 2150000.mmc: Removing from iommu group 12 fsl-edma 22c0000.dma-controller: Removing from iommu group 17 dwc3 3100000.usb: Removing from iommu group 9 dwc3 3110000.usb: Removing from iommu group 10 ahci-qoriq 3200000.sata: Removing from iommu group 2 fsl-qdma 8380000.dma-controller: Removing from iommu group 20 platform f080000.display: Removing from iommu group 0 etnaviv-gpu f0c0000.gpu: Removing from iommu group 1 etnaviv etnaviv: Removing from iommu group 1 caam_jr 8010000.jr: Removing from iommu group 13 caam_jr 8020000.jr: Removing from iommu group 14 caam_jr 8030000.jr: Removing from iommu group 15 caam_jr 8040000.jr: Removing from iommu group 16 fsl_enetc 0000:00:00.0: Removing from iommu group 4 arm-smmu 5000000.iommu: Blocked unknown Stream ID 0x429; boot with "arm-smmu.disable_bypass=0" to allow, but this may have security implications arm-smmu 5000000.iommu: GFSR 0x80000002, GFSYNR0 0x00000002, GFSYNR1 0x00000429, GFSYNR2 0x00000000 fsl_enetc 0000:00:00.1: Removing from iommu group 5 arm-smmu 5000000.iommu: Blocked unknown Stream ID 0x429; boot with "arm-smmu.disable_bypass=0" to allow, but this may have security implications arm-smmu 5000000.iommu: GFSR 0x80000002, GFSYNR0 0x00000002, GFSYNR1 0x00000429, GFSYNR2 0x00000000 arm-smmu 5000000.iommu: Blocked unknown Stream ID 0x429; boot with "arm-smmu.disable_bypass=0" to allow, but this may have security implications arm-smmu 5000000.iommu: GFSR 0x80000002, GFSYNR0 0x00000000, GFSYNR1 0x00000429, GFSYNR2 0x00000000 fsl_enetc 0000:00:00.2: Removing from iommu group 6 fsl_enetc_mdio 0000:00:00.3: Removing from iommu group 8 mscc_felix 0000:00:00.5: Removing from iommu group 3 fsl_enetc 0000:00:00.6: Removing from iommu group 7 pcieport 0001:00:00.0: Removing from iommu group 18 arm-smmu 5000000.iommu: Blocked unknown Stream ID 0x429; boot with "arm-smmu.disable_bypass=0" to allow, but this may have security implications arm-smmu 5000000.iommu: GFSR 0x00000002, GFSYNR0 0x00000000, GFSYNR1 0x00000429, GFSYNR2 0x00000000 pcieport 0002:00:00.0: Removing from iommu group 19 Unable to handle kernel NULL pointer dereference at virtual address 00000000000000a8 pc : iommu_get_dma_domain+0x14/0x20 lr : iommu_dma_unmap_page+0x38/0xe0 Call trace: iommu_get_dma_domain+0x14/0x20 dma_unmap_page_attrs+0x38/0x1d0 en ---truncated---	5.5	More Details
CVE-2022-48894	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu-v3: Don't unregister on shutdown Similar to SMMUv2, this driver calls iommu_device_unregister() from the shutdown path, which removes the IOMMU groups with no coordination whatsoever with their users - shutdown methods are optional in device drivers. This can lead to NULL pointer dereferences in those drivers' DMA API calls, or worse. Instead of calling the full arm_smmu_device_remove() from arm_smmu_device_shutdown(), let's pick only the relevant function call - arm_smmu_device_disable() - more or less the reverse of arm_smmu_device_reset() - and call just that from the shutdown path.	5.5	More Details
CVE-2022-48893	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Cleanup partial engine discovery failures If we abort driver initialisation in the middle of gt/engine discovery, some engines will be fully setup and some not. Those incompletely setup engines only have 'engine->release == NULL' and so will leak any of the common objects allocated. v2: - Drop the destroy_pinned_context() helper for now. It's not really worth it with just a single callsite at the moment. (Janusz)	5.5	More Details
CVE-2022-48891	In the Linux kernel, the following vulnerability has been resolved: regulator: da9211: Use irq handler when ready If the system does not come from reset (like when it is kexec()), the regulator might have an IRQ waiting for us. If we enable the IRQ handler before its structures are ready, we crash. This patch fixes: [1.141839] Unable to handle kernel read from unreadable memory at virtual address 0000000000000078 [1.316096] Call trace: [1.316101] blocking_notifier_call_chain+0x20/0xa8 [1.322757] cpu cpu0: dummy supplies not allowed for exclusive requests [1.327823] regulator_notifier_call_chain+0x1c/0x2c [1.327825] da9211_irq_handler+0x68/0xf8 [1.327829] irq_thread+0x11c/0x234 [1.327833] kthread+0x13c/0x154	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48882	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix macsec possible null dereference when updating MAC security entity (SecY) Upon updating MAC security entity (SecY) in hw offload path, the macsec security association (SA) initialization routine is called. In case of extended packet number (epn) is enabled the salt and ssci attributes are retrieved using the MACsec driver rx_sa context which is unavailable when updating a SecY property such as encoding-sa hence the null dereference. Fix by using the provided SA to set those attributes.	5.5	More Details
CVE-2022-48890	In the Linux kernel, the following vulnerability has been resolved: scsi: storvsc: Fix swiotlb bounce buffer leak in confidential VM storvsc_queuecommand() maps the scatter/gather list using scsi_dma_map(), which in a confidential VM allocates swiotlb bounce buffers. If the I/O submission fails in storvsc_do_io(), the I/O is typically retried by higher level code, but the bounce buffer memory is never freed. The mostly like cause of I/O submission failure is a full VMBus channel ring buffer, which is not uncommon under high I/O loads. Eventually enough bounce buffer memory leaks that the confidential VM can't do any I/O. The same problem can arise in a non-confidential VM with kernel boot parameter swiotlb=force. Fix this by doing scsi_dma_unmap() in the case of an I/O submission error, which frees the bounce buffer memory.	5.5	More Details
CVE-2024-43915	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dylan James Zephyr Project Manager allows Reflected XSS.This issue affects Zephyr Project Manager: from n/a through .3.102.	5.5	More Details
CVE-2022-48885	In the Linux kernel, the following vulnerability has been resolved: ice: Fix potential memory leak in ice_gnss_tty_write() The ice_gnss_tty_write() return directly if the write_buf alloc failed, leaking the cmd_buf. Fix by free cmd_buf if write_buf alloc failed.	5.5	More Details
CVE-2022-48886	In the Linux kernel, the following vulnerability has been resolved: ice: Add check for kzalloc Add the check for the return value of kzalloc in order to avoid NULL pointer dereference. Moreover, use the goto-label to share the clean code.	5.5	More Details
CVE-2022-48887	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Remove rcu locks from user resources User resource lookups used rcu to avoid two extra atomics. Unfortunately the rcu paths were buggy and it was easy to make the driver crash by submitting command buffers from two different threads. Because the lookups never show up in performance profiles replace them with a regular spin lock which fixes the races in accesses to those shared resources. Fixes kernel oops'es in IGT's vmwgfx execution_buffer stress test and seen crashes with apps using shared resources.	5.5	More Details
CVE-2023-52894	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ncm: fix potential NULL ptr deref in ncm_bitrate() In Google internal bug 265639009 we've received an (as yet) unreproducible crash report from an aarch64 GKI 5.10.149-android13 running device. AFAICT the source code is at: https://android.googlesource.com/kernel/common/+/refs/tags/ASB-2022-12-05_13-5.10 The call stack is: ncm_close() -> ncm_notify() -> ncm_do_notify() with the crash at: ncm_do_notify+0x98/0x270 Code: 79000d0b b9000a6c f940012a f9400269 (b9405d4b) Which I believe disassembles to (I don't know ARM assembly, but it looks sane enough to me...): // halfword (16-bit) store presumably to event->wLength (at offset 6 of struct usb_cdc_notification) 0B 0D 00 79 strh w11, [x8, #6] // word (32-bit) store presumably to req->Length (at offset 8 of struct usb_request) 6C 0A 00 B9 str w12, [x19, #8] // x10 (NULL) was read here from offset 0 of valid pointer x9 // IMHO we're reading 'cdev->gadget' and getting NULL // gadget is indeed at offset 0 of struct usb_composite_dev 2A 01 40 F9 ldr x10, [x9] // loading req->buf pointer, which is at offset 0 of struct usb_request 69 02 40 F9 ldr x9, [x19] // x10 is null, crash, appears to be attempt to read cdev->gadget->max_speed 4B 5D 40 B9 ldr w11, [x10, #0x5c] which seems to line up with ncm_do_notify() case NCM_NOTIFY_SPEED code fragment: event->wLength = cpu_to_le16(8); req->length = NCM_STATUS_BYTECOUNT; /* SPEED_CHANGE data is up/down speeds in bits/sec */ data = req->buf + sizeof *event; data[0] = cpu_to_le32(ncm_bitrate(cdev->gadget)); My analysis of registers and NULL ptr deref crash offset (Unable to handle kernel NULL pointer dereference at virtual address 000000000000005c) heavily suggests that the crash is due to 'cdev->gadget' being NULL when executing: data[0] = cpu_to_le32(ncm_bitrate(cdev->gadget)); which calls: ncm_bitrate(NULL) which then calls: gadget_is_superspeed(NULL) which reads ((struct usb_gadget *)NULL)->max_speed and hits a panic. AFAICT, if I'm counting right, the offset of max_speed is indeed 0x5C. (remember there's a GKI KABI reservation of 16 bytes in struct work_struct) It's not at all clear to me how this is all supposed to work... but returning 0 seems much better than panic-ing...	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48876	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix initialization of rx->link and rx->link_sta There are some codepaths that do not initialize rx->link_sta properly. This causes a crash in places which assume that rx->link_sta is valid if rx->sta is valid. One known instance is triggered by __ieee80211_rx_h_amsdu being called from fast-rx. It results in a crash like this one: BUG: kernel NULL pointer dereference, address: 00000000000000a8 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] PREEMPT SMP PTI CPU: 1 PID: 506 Comm: mt76-usb-rx phy Tainted: G E 6.1.0-debian64x+1.7 #3 Hardware name: ZOTAC ZBOX-ID92/ZBOX-IQ01/ZBOX-ID92/ZBOX-IQ01, BIOS B220P007 05/21/2014 RIP: 0010:ieee80211_deliver_skb+0x62/0x1f0 [mac80211] Code: 00 48 89 04 24 e8 9e a7 c3 df 89 c0 48 03 1c c5 a0 ea 39 a1 4c 01 6b 08 48 ff 03 48 83 7d 28 00 74 11 48 8b 45 30 48 63 55 44 <48> 83 84 d0 a8 00 00 00 01 41 8b 86 c0 11 00 00 8d 50 fd 83 fa 01 RSP: 0018:ffff999040803b10 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffffb9903f496480 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff999040803ce0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8d21828ac900 R13: 000000000000004a R14: ffff8d2198ed89c0 R15: ffff8d2198ed8000 FS: 0000000000000000(0000) GS:ffff8d24afe80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000000000a8 CR3: 0000000429810002 CR4: 0000000001706e0 Call Trace: <TASK> __ieee80211_rx_h_amsdu+0x1b5/0x240 [mac80211] ? ieee80211_prepare_and_rx_handle+0xcdd/0x1320 [mac80211] ? __local_bh_enable_ip+0x3b/0xa0 ieee80211_prepare_and_rx_handle+0xcdd/0x1320 [mac80211] ? prepare_transfer+0x109/0x1a0 [xhci_hcd] ieee80211_rx_list+0xa80/0xda0 [mac80211] mt76_rx_complete+0x207/0x2e0 [mt76] mt76_rx_poll_complete+0x357/0x5a0 [mt76] mt76u_rx_worker+0x4f5/0x600 [mt76_usb] ? mt76_get_min_avg_rssi+0x140/0x140 [mt76] __mt76_worker_fn+0x50/0x80 [mt76] kthread+0xed/0x120 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x22/0x30 Since the initialization of rx->link and rx->link_sta is rather convoluted and duplicated in many places, clean it up by using a helper function to set it. [remove unnecessary rx->sta->sta.mlo check]	5.5	More Details
CVE-2022-48888	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: Fix memory leak in msm_mdss_parse_data_bus_icc_path of_icc_get() alloc resources for path1, we should release it when not need anymore. Early return when IS_ERR_OR_NULL(path0) may leak path1. Defer getting path1 to fix this. Patchwork: https://patchwork.freedesktop.org/patch/514264/	5.5	More Details
CVE-2024-41175	The IPC-Diagnostics package included in TwinCAT/BSD is vulnerable to a local denial-of-service attack by a low privileged attacker.	5.5	More Details
CVE-2024-43913	In the Linux kernel, the following vulnerability has been resolved: nvme: apple: fix device reference counting Drivers must call nvme_uninit_ctrl after a successful nvme_init_ctrl. Split the allocation side out to make the error handling boundary easier to navigate. The apple driver had been doing this wrong, leaking the controller device memory on a tagset failure.	5.5	More Details
CVE-2024-43914	In the Linux kernel, the following vulnerability has been resolved: md/raid5: avoid BUG_ON() while continue reshape after reassembling Currently, mdadm support --revert-reshape to abort the reshape while reassembling, as the test 07revert-grow. However, following BUG_ON() can be triggerred by the test: kernel BUG at drivers/md/raid5.c:6278! invalid opcode: 0000 [#1] PREEMPT SMP PTI irq event stamp: 158985 CPU: 6 PID: 891 Comm: md0_reshape Not tainted 6.9.0-03335-g7592a0b0049a #94 RIP: 0010:reshape_request+0x3f1/0xe60 Call Trace: <TASK> raid5_sync_request+0x43d/0x550 md_do_sync+0xb7a/0x2110 md_thread+0x294/0x2b0 kthread+0x147/0x1c0 ret_from_fork+0x59/0x70 ret_from_fork_asm+0x1a/0x30 </TASK> Root cause is that --revert-reshape update the raid_disks from 5 to 4, while reshape position is still set, and after reassembling the array, reshape position will be read from super block, then during reshape the checking of 'writepos' that is caculated by old reshape position will fail. Fix this panic the easy way first, by converting the BUG_ON() to WARN_ON(), and stop the reshape if checkings fail. Noted that mdadm must fix --revert-shape as well, and probably md/raid should enhance metadata validation as well, however this means reassemble will fail and there must be user tools to fix the wrong metadata.	5.5	More Details
CVE-2024-44931	In the Linux kernel, the following vulnerability has been resolved: gpio: prevent potential speculation leaks in gpio_device_get_desc() Userspace may trigger a speculative read of an address outside the gpio descriptor array. Users can do that by calling gpio_ioctl() with an offset out of range. Offset is copied from user and then used as an array index to get the gpio descriptor without sanitization in gpio_device_get_desc(). This change ensures that the offset is sanitized by using array_index_nospec() to mitigate any possibility of speculative information leaks. This bug was discovered and resolved using Coverity Static Analysis Security Testing (SAST) by Synopsys, Inc.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52903	In the Linux kernel, the following vulnerability has been resolved: io_uring: lock overflowing for IOPOLL syzbot reports an issue with overflow filling for IOPOLL: WARNING: CPU: 0 PID: 28 at io_uring/io_uring.c:734 io_cqring_event_overflow+0x1c0/0x230 io_uring/io_uring.c:734 CPU: 0 PID: 28 Comm: kworker/u4:1 Not tainted 6.2.0-rc3-syzkaller-16369-g358a161a6a9e #0 Workqueue: events_unbound io_ring_exit_work Call trace: io_cqring_event_overflow+0x1c0/0x230 io_uring/io_uring.c:734 io_req_cqe_overflow+0x5c/0x70 io_uring/io_uring.c:773 io_fill_cqe_req io_uring/io_uring.h:168 [inline] io_do_iopoll+0x474/0x62c io_uring/rw.c:1065 io_iopoll_try_reap_events+0x6c/0x108 io_uring/io_uring.c:1513 io_uring_try_cancel_requests+0x13c/0x258 io_uring/io_uring.c:3056 io_ring_exit_work+0xec/0x390 io_uring/io_uring.c:2869 process_one_work+0x2d8/0x504 kernel/workqueue.c:2289 worker_thread+0x340/0x610 kernel/workqueue.c:2436 kthread+0x12c/0x158 kernel/kthread.c:376 ret_from_fork+0x10/0x20 arch/arm64/kernel/entry.S:863 There is no real problem for normal IOPOLL as flush is also called with uring_lock taken, but it's getting more complicated for IOPOLLISQPOLL, for which __io_cqring_overflow_flush() happens from the CQ waiting path.	5.5	More Details
CVE-2024-44933	In the Linux kernel, the following vulnerability has been resolved: bnxt_en : Fix memory out-of-bounds in bnxt_fill_hw_rss_tbl() A recent commit has modified the code in __bnxt_reserve_rings() to set the default RSS indirection table to default only when the number of RX rings is changing. While this works for newer firmware that requires RX ring reservations, it causes the regression on older firmware not requiring RX ring resrvations (BNXT_NEW_RM() returns false). With older firmware, RX ring reservations are not required and so hw_resc->resv_rx_rings is not always set to the proper value. The comparison: if (old_rx_rings != bp->hw_resc.resv_rx_rings) in __bnxt_reserve_rings() may be false even when the RX rings are changing. This will cause __bnxt_reserve_rings() to skip setting the default RSS indirection table to default to match the current number of RX rings. This may later cause bnxt_fill_hw_rss_tbl() to use an out-of-range index. We already have bnxt_check_rss_tbl_no_rmgr() to handle exactly this scenario. We just need to move it up in bnxt_need_reserve_rings() to be called unconditionally when using older firmware. Without the fix, if the TX rings are changing, we'll skip the bnxt_check_rss_tbl_no_rmgr() call and __bnxt_reserve_rings() may also skip the bnxt_set_dflt_rss_indir_tbl() call for the reason explained in the last paragraph. Without setting the default RSS indirection table to default, it causes the regression: BUG: KASAN: slab-out-of-bounds in __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 Read of size 2 at addr ffff8881c5809618 by task ethtool/31525 Call Trace: __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 bnxt_hwrm_vnic_rss_cfg_p5+0xf7/0x460 __bnxt_setup_vnic_p5+0x12e/0x270 __bnxt_open_nic+0x2262/0x2f30 bnxt_open_nic+0x5d/0xf0 ethnl_set_channels+0x5d4/0xb30 ethnl_default_set_doit+0x2f1/0x620	5.5	More Details
CVE-2023-52902	In the Linux kernel, the following vulnerability has been resolved: nommu: fix memory leak in do_mmap() error path The preallocation of the maple tree nodes may leak if the error path to "error_just_free" is taken. Fix this by moving the freeing of the maple tree nodes to a shared location for all error paths.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44935	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_sock() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint(). [0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89 f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 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: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 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 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0 R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated---	5.5	More Details
CVE-2024-44936	In the Linux kernel, the following vulnerability has been resolved: power: supply: rt5033: Bring back i2c_set_clientdata Commit 3a93da231c12 ("power: supply: rt5033: Use devm_power_supply_register() helper") reworked the driver to use devm. While at it, the i2c_set_clientdata was dropped along with the remove callback. Unfortunately other parts of the driver also rely on i2c clientdata so this causes kernel oops. Bring the call back to fix the driver.	5.5	More Details
CVE-2024-44937	In the Linux kernel, the following vulnerability has been resolved: platform/x86: intel-vbtn: Protect ACPI notify handler against recursion Since commit e2ffcda16290 ("ACPI: OSL: Allow Notify () handlers to run on all CPUs") ACPI notify handlers like the intel-vbtn notify_handler() may run on multiple CPU cores racing with themselves. This race gets hit on Dell Venue 7140 tablets when undocking from the keyboard, causing the handler to try and register priv->switches_dev twice, as can be seen from the dev_info() message getting logged twice: [83.861800] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event [83.861858] input: Intel Virtual Switches as /devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17 [83.861865] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event After which things go seriously wrong: [83.861872] sysfs: cannot create duplicate filename '/devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17' ... [83.861967] kobject: kobject_add_internal failed for input17 with -EEXIST, don't try to register things with the same name in the same directory. [83.877338] BUG: kernel NULL pointer dereference, address: 0000000000000018 ... Protect intel-vbtn notify_handler() from racing with itself with a mutex to fix this.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52901	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Check endpoint is valid before dereferencing it When the host controller is not responding, all URBs queued to all endpoints need to be killed. This can cause a kernel panic if we dereference an invalid endpoint. Fix this by using xhci_get_virt_ep() helper to find the endpoint and checking if the endpoint is valid before dereferencing it. [233311.853271] xhci-hcd xhci-hcd.1.auto: xHCI host controller not responding, assume dead [233311.853393] Unable to handle kernel NULL pointer dereference at virtual address 00000000000000e8 [233311.853964] pc : xhci_hc_died+0x10c/0x270 [233311.853971] lr : xhci_hc_died+0x1ac/0x270 [233311.854077] Call trace: [233311.854085] xhci_hc_died+0x10c/0x270 [233311.854093] xhci_stop_endpoint_command_watchdog+0x100/0x1a4 [233311.854105] call_timer_fn+0x50/0x2d4 [233311.854112] expire_timers+0xac/0x2e4 [233311.854118] run_timer_softirq+0x300/0xabc [233311.854127] __do_softirq+0x148/0x528 [233311.854135] irq_exit+0x194/0x1a8 [233311.854143] __handle_domain_irq+0x164/0x1d0 [233311.854149] gic_handle_irq.22273+0x10c/0x188 [233311.854156] el1_irq+0xfc/0x1a8 [233311.854175] lpm_cpuidle_enter+0x25c/0x418 [msm_pm] [233311.854185] cpuidle_enter_state+0x1f0/0x764 [233311.854194] do_idle+0x594/0x6ac [233311.854201] cpu_startup_entry+0x7c/0x80 [233311.854209] secondary_start_kernel+0x170/0x198	5.5	More Details
CVE-2023-52900	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix general protection fault in nilfs_btree_insert() If nilfs2 reads a corrupted disk image and tries to reads a b-tree node block by calling __nilfs_btree_get_block() against an invalid virtual block address, it returns -ENOENT because conversion of the virtual block address to a disk block address fails. However, this return value is the same as the internal code that b-tree lookup routines return to indicate that the block being searched does not exist, so functions that operate on that b-tree may misbehave. When nilfs_btree_insert() receives this spurious 'not found' code from nilfs_btree_do_lookup(), it misunderstands that the 'not found' check was successful and continues the insert operation using incomplete lookup path data, causing the following crash: general protection fault, probably for non-canonical address 0xdffffc0000000005: 0000 [#1] PREEMPT SMP KASAN KASAN: null-ptr-deref in range [0x0000000000000028-0x000000000000002f] ... RIP: 0010:nilfs_btree_get_nonroot_node fs/nilfs2/btree.c:418 [inline] RIP: 0010:nilfs_btree_prepare_insert fs/nilfs2/btree.c:1077 [inline] RIP: 0010:nilfs_btree_insert+0x6d3/0x1c10 fs/nilfs2/btree.c:1238 Code: bc 24 80 00 00 00 4c 89 f8 48 c1 e8 03 42 80 3c 28 00 74 08 4c 89 ff e8 4b 02 92 fe 4d 8b 3f 49 83 c7 28 4c 89 f8 48 c1 e8 03 <42> 80 3c 28 00 74 08 4c 89 ff e8 2e 02 92 fe 4d 8b 3f 49 83 c7 02 ... Call Trace: <TASK> nilfs_bmap_do_insert fs/nilfs2/bmap.c:121 [inline] nilfs_bmap_insert+0x20d/0x360 fs/nilfs2/bmap.c:147 nilfs_get_block+0x414/0x8d0 fs/nilfs2/inode.c:101 __block_write_begin_int+0x54c/0x1a80 fs/buffer.c:1991 __block_write_begin fs/buffer.c:2041 [inline] block_write_begin+0x93/0x1e0 fs/buffer.c:2102 nilfs_write_begin+0x9c/0x110 fs/nilfs2/inode.c:261 generic_perform_write+0x2e4/0x5e0 mm/filemap.c:3772 __generic_file_write_iter+0x176/0x400 mm/filemap.c:3900 generic_file_write_iter+0xab/0x310 mm/filemap.c:3932 call_write_iter include/linux/fs.h:2186 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x7dc/0xc50 fs/read_write.c:584 ksys_write+0x177/0x2a0 fs/read_write.c:637 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd ... </TASK> This patch fixes the root cause of this problem by replacing the error code that __nilfs_btree_get_block() returns on block address conversion failure from -ENOENT to another internal code -EINVAL which means that the b-tree metadata is corrupted. By returning -EINVAL, it propagates without glitches, and for all relevant b-tree operations, functions in the upper bmap layer output an error message indicating corrupted b-tree metadata via nilfs_bmap_convert_error(), and code -EIO will be eventually returned as it should be.	5.5	More Details
CVE-2024-44938	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix shift-out-of-bounds in dbDiscardAG When searching for the next smaller log2 block, BLKSTOL2() returned 0, causing shift exponent -1 to be negative. This patch fixes the issue by exiting the loop directly when negative shift is found.	5.5	More Details
CVE-2024-44939	In the Linux kernel, the following vulnerability has been resolved: jfs: fix null ptr deref in dtInsertEntry [syzbot reported] general protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f] CPU: 0 PID: 5061 Comm: syz-executor404 Not tainted 6.8.0-syzkaller-08951-gfe46a7dd189e #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:dtInsertEntry+0xd0c/0x1780 fs/jfs/jfs_dtree.c:3713 ... [Analyze] In dtInsertEntry(), when the pointer h has the same value as p, after writing name in UniStrncpy_to_le(), p->header.flag will be cleared. This will cause the previously true judgment "p->header.flag & BT-LEAF" to change to no after writing the name operation, this leads to entering an incorrect branch and accessing the uninitialized object ih when judging this condition for the second time. [Fix] After got the page, check freelist first, if freelist == 0 then exit dtInsert() and return -EINVAL.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52899	In the Linux kernel, the following vulnerability has been resolved: Add exception protection processing for vd in axi_chan_handle_err function Since there is no protection for vd, a kernel panic will be triggered here in exceptional cases. You can refer to the processing of axi_chan_block_xfer_complete function The triggered kernel panic is as follows: [67.848444] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000060 [67.848447] Mem abort info: [67.848449] ESR = 0x96000004 [67.848451] EC = 0x25: DABT (current EL), IL = 32 bits [67.848454] SET = 0, FnV = 0 [67.848456] EA = 0, S1PTW = 0 [67.848458] Data abort info: [67.848460] ISV = 0, ISS = 0x00000004 [67.848462] CM = 0, WnR = 0 [67.848465] user pgtable: 4k pages, 48-bit VAs, pgdp=00000800c4c0b000 [67.848468] [0000000000000060] pgd=0000000000000000, p4d=0000000000000000 [67.848472] Internal error: Oops: 96000004 [#1] SMP [67.848475] Modules linked in: dmatest [67.848479] CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.10.100-emu_x2rc+ #11 [67.848483] pstate: 62000085 (nZCv daIf -PAN -UAO +TCO BTYPE=--) [67.848487] pc : axi_chan_handle_err+0xc4/0x230 [67.848491] lr : axi_chan_handle_err+0x30/0x230 [67.848493] sp : ffff0803fe55ae50 [67.848495] x29: ffff0803fe55ae50 x28: ffff800011212200 [67.848500] x27: ffff0800c42c0080 x26: ffff0800c097c080 [67.848504] x25: ffff800010d33880 x24: ffff80001139d850 [67.848508] x23: ffff0800c097c168 x22: 0000000000000000 [67.848512] x21: 0000000000000080 x20: 0000000000002000 [67.848517] x19: ffff0800c097c080 x18: 0000000000000000 [67.848521] x17: 0000000000000000 x16: 0000000000000000 [67.848525] x15: 0000000000000000 x14: 0000000000000000 [67.848529] x13: 0000000000000000 x12: 0000000000000040 [67.848533] x11: ffff0800c0400248 x10: ffff0800c040024a [67.848538] x9 : ffff800010576cd4 x8 : ffff0800c0400270 [67.848542] x7 : 0000000000000000 x6 : ffff0800c04003e0 [67.848546] x5 : ffff0800c0400248 x4 : ffff0800c4294480 [67.848550] x3 : dead000000000100 x2 : dead000000000122 [67.848555] x1 : 0000000000000100 x0 : ffff0800c097c168 [67.848559] Call trace: [67.848562] axi_chan_handle_err+0xc4/0x230 [67.848566] dw_axi_dma_interrupt+0xf4/0x590 [67.848569] __handle_irq_event_percpu+0x60/0x220 [67.848573] handle_irq_event+0x64/0x120 [67.848576] handle_fasteoi_irq+0xc4/0x220 [67.848580] __handle_domain_irq+0x80/0xe0 [67.848583] gic_handle_irq+0xc0/0x138 [67.848585] el1_irq+0xc8/0x180 [67.848588] arch_cpu_idle+0x14/0x2c [67.848591] default_idle_call+0x40/0x16c [67.848594] do_idle+0x1f0/0x250 [67.848597] cpu_startup_entry+0x2c/0x60 [67.848600] rest_init+0xc0/0xcc [67.848603] arch_call_rest_init+0x14/0x1c [67.848606] start_kernel+0x4cc/0x500 [67.848610] Code: eb0002ff 9a9f12d6 f2fbd5a2 f2fbd5a3 (a94602c1) [67.848613] ---[end trace 585a97036f88203a]---	5.5	More Details
CVE-2022-48875	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: sdata can be NULL during AMPDU start ieee80211_tx_ba_session_handle_start() may get NULL for sdata when a deauthentication is ongoing. Here a trace triggering the race with the hostapd test multi_ap_fronthaul_on_ap: (gdb) list *drv_ampdu_action+0x46 0x8b16 is in drv_ampdu_action (net/mac80211/driver-ops.c:396). 391 int ret = -EOPNOTSUPP; 392 393 might_sleep(); 394 395 sdata = get_bss_sdata(sdata); 396 if (!check_sdata_in_driver(sdata)) 397 return -EIO; 398 399 trace_drv_ampdu_action(local, sdata, params); 400 wlan0: moving STA 02:00:00:00:03:00 to state 3 wlan0: associated wlan0: deauthenticating from 02:00:00:00:03:00 by local choice (Reason: 3=DEAUTH_LEAVING) wlan3.sta1: Open BA session requested for 02:00:00:00:00:00 tid 0 wlan3.sta1: dropped frame to 02:00:00:00:00:00 (unauthorized port) wlan0: moving STA 02:00:00:00:03:00 to state 2 wlan0: moving STA 02:00:00:00:03:00 to state 1 wlan0: Removed STA 02:00:00:00:03:00 wlan0: Destroyed STA 02:00:00:00:03:00 BUG: unable to handle page fault for address: ffffffffffffffb48 PGD 11814067 P4D 11814067 PUD 11816067 PMD 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 2 PID: 133397 Comm: kworker/u16:1 Tainted: G W 6.1.0-rc8-wt+ #59 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.0-20220807_005459-localhost 04/01/2014 Workqueue: phy3 ieee80211_ba_session_work [mac80211] RIP: 0010:drv_ampdu_action+0x46/0x280 [mac80211] Code: 53 48 89 f3 be 89 01 00 00 e8 d6 43 bf ef e8 21 46 81 f0 83 bb a0 1b 00 00 04 75 0e 48 8b 9b 28 0d 00 00 48 81 eb 10 0e 00 00 <8b> 93 58 09 00 00 f6 c2 20 0f 84 3b 01 00 00 8b 05 dd 1c 0f 00 85 RSP: 0018:ffffc900025ebd20 EFLAGS: 00010287 RAX: 0000000000000000 RBX: ffffffffffffff1f0 RCX: ffff888102228240 RDX: 0000000080000000 RSI: ffffffff918c5de0 RDI: ffff888102228b40 RBP: ffffc900025ebd40 R08: 0000000000000001 R09: 0000000000000001 R10: 0000000000000001 R11: 0000000000000000 R12: ffff888118c18ec0 R13: 0000000000000000 R14: ffffc900025ebd60 R15: ffff888018b7efb8 FS: 0000000000000000(0000) GS:ffff88817a600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffffffffb48 CR3: 0000000105228006 CR4: 0000000000170ee0 Call Trace: <TASK> ieee80211_tx_ba_session_handle_start+0xd0/0x190 [mac80211] ieee80211_ba_session_work+0xff/0x2e0 [mac80211] process_one_work+0x29f/0x620 worker_thread+0x4d/0x3d0 ? process_one_work+0x620/0x620 kthread+0xfb/0x120 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x22/0x30 </TASK>	5.5	More Details
CVE-2023-49582	Lax permissions set by the Apache Portable Runtime library on Unix platforms would allow local users read access to named shared memory segments, potentially revealing sensitive application data. This issue does not affect non-Unix platforms, or builds with APR_USE_SHMEM_SHMGET=1 (apr.h) Users are recommended to upgrade to APR version 1.7.5, which fixes this issue.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52905	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: Fix resource leakage in VF driver unbind resources allocated like mcam entries to support the Ntuple feature and hash tables for the tc feature are not getting freed in driver unbind. This patch fixes the issue.	5.5	More Details
CVE-2024-43862	In the Linux kernel, the following vulnerability has been resolved: net: wan: fsl_qmc_hdlc: Convert carrier_lock spinlock to a mutex The carrier_lock spinlock protects the carrier detection. While it is held, framer_get_status() is called which in turn takes a mutex. This is not correct and can lead to a deadlock. A run with PROVE_LOCKING enabled detected the issue: [BUG: Invalid wait context] ... c204ddbc (&framer->mutex){+.+.}-{3:3}, at: framer_get_status+0x40/0x78 other info that might help us debug this: context-{4:4} 2 locks held by ifconfig/146: #0: c0926a38 (rtnl_mutex){+.+.}-{3:3}, at: devinet_ioctl+0x12c/0x664 #1: c2006a40 (&qmc_hdlc->carrier_lock){....}-{2:2}, at: qmc_hdlc_framer_set_carrier+0x30/0x98 Avoid the spinlock usage and convert carrier_lock to a mutex.	5.5	More Details
CVE-2022-48924	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly.	5.5	More Details
CVE-2022-48922	In the Linux kernel, the following vulnerability has been resolved: riscv: fix oops caused by irqsoff latency tracer The trace_hardirqs_{on,off}() require the caller to setup frame pointer properly. This because these two functions use macro 'CALLER_ADDR1' (aka. __builtin_return_address(1)) to acquire caller info. If the $fp is used for other purpose, the code generated this macro (as below) could trigger memory access fault. 0xffffffff8011510e <+80>: ld a1,-16(s0) 0xffffffff80115112 <+84>: ld s2,-8(a1) # <-- paging fault here The oops message during booting if compiled with 'irqoff' tracer enabled: [0.039615][T0] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000f8 [0.041925][T0] Oops [#1] [0.042063][T0] Modules linked in: [0.042864][T0] CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.17.0-rc1-00233-g9a20c48d1ed2 #29 [0.043568][T0] Hardware name: riscv-virtio,qemu (DT) [0.044343][T0] epc : trace_hardirqs_on+0x56/0xe2 [0.044601][T0] ra : restore_all+0x12/0x6e [0.044721][T0] epc : ffffffff80126a5c ra : ffffffff80003b94 sp : ffffffff81403db0 [0.044801][T0] gp : ffffffff8163acd8 tp : ffffffff81414880 t0 : 0000000000000020 [0.044882][T0] t1 : 0098968000000000 t2 : 0000000000000000 s0 : ffffffff81403de0 [0.044967][T0] s1 : 0000000000000000 a0 : 0000000000000001 a1 : 0000000000000100 [0.045046][T0] a2 : 0000000000000000 a3 : 0000000000000000 a4 : 0000000000000000 [0.045124][T0] a5 : 0000000000000000 a6 : 0000000000000000 a7 : 0000000054494d45 [0.045210][T0] s2 : ffffffff80003b94 s3 : ffffffff81a8f1b0 s4 : ffffffff80e27b50 [0.045289][T0] s5 : ffffffff81414880 s6 : ffffffff8160fa00 s7 : 00000000800120e8 [0.045389][T0] s8 : 0000000080013100 s9 : 000000000000007f s10: 0000000000000000 [0.045474][T0] s11: 0000000000000000 t3 : 7fffffffffffffff t4 : 0000000000000000 [0.045548][T0] t5 : 0000000000000000 t6 : ffffffff814aa368 [0.045620][T0] status: 0000000200000100 badaddr: 00000000000000f8 cause: 000000000000000d [0.046402][T0] [<ffffffff80003b94>] restore_all+0x12/0x6e This because the $fp(aka. $s0) register is not used as frame pointer in the assembly entry code. resume_kernel: REG_L s0, TASK_TI_PREEMPT_COUNT(tp) bnez s0, restore_all REG_L s0, TASK_TI_FLAGS(tp) andi s0, s0, _TIF_NEED_RESCHED beqz s0, restore_all call preempt_schedule_irq j restore_all To fix above issue, here we add one extra level wrapper for function trace_hardirqs_{on,off}() so they can be safely called by low level entry code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48920	In the Linux kernel, the following vulnerability has been resolved: btrfs: get rid of warning on transaction commit when using flushoncommit When using the flushoncommit mount option, during almost every transaction commit we trigger a warning from __writeback_inodes_sb_nr(): $ cat fs/fs-writeback.c: (...) static void __writeback_inodes_sb_nr(struct super_block *sb, ... { (...) WARN_ON(!rwsem_is_locked(&sb->s_umount)); (...) } (...) The trace produced in dmesg looks like the following: [947.473890] WARNING: CPU: 5 PID: 930 at fs/fs-writeback.c:2610 __writeback_inodes_sb_nr+0x7e/0xb3 [947.481623] Modules linked in: nfsd nls_cp437 cifs asn1_decoder cifs_arc4 fscache cifs_md4 ipmi_ssif [947.489571] CPU: 5 PID: 930 Comm: btrfs-transacti Not tainted 95.16.3-srb-asrock-00001-g36437ad63879 #186 [947.497969] RIP: 0010:__writeback_inodes_sb_nr+0x7e/0xb3 [947.502097] Code: 24 10 4c 89 44 24 18 c6 (...) [947.519760] RSP: 0018:ffffc90000777e10 EFLAGS: 00010246 [947.523818] RAX: 0000000000000000 RBX: 0000000000963300 RCX: 0000000000000000 [947.529765] RDX: 0000000000000000 RSI: 000000000000fa51 RDI: ffffc90000777e50 [947.535740] RBP: ffff888101628a90 R08: ffff888100955800 R09: ffff888100956000 [947.541701] R10: 0000000000000002 R11: 0000000000000001 R12: ffff888100963488 [947.547645] R13: ffff888100963000 R14: ffff888112fb7200 R15: ffff888100963460 [947.553621] FS: 0000000000000000(0000) GS:ffff88841fd40000(0000) knlGS:0000000000000000 [947.560537] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [947.565122] CR2: 0000000008be50c4 CR3: 000000000220c000 CR4: 00000000001006e0 [947.571072] Call Trace: [947.572354] <TASK> [947.573266] btrfs_commit_transaction+0x1f1/0x998 [947.576785] ? start_transaction+0x3ab/0x44e [947.579867] ? schedule_timeout+0x8a/0xdd [947.582716] transaction_kthread+0xe9/0x156 [947.585721] ? btrfs_cleanup_transaction.isra.0+0x407/0x407 [947.590104] kthread+0x131/0x139 [947.592168] ? set_kthread_struct+0x32/0x32 [947.595174] ret_from_fork+0x22/0x30 [947.597561] </TASK> [947.598553] ---[end trace 644721052755541c]--- This is because we started using writeback_inodes_sb() to flush delalloc when committing a transaction (when using -o flushoncommit), in order to avoid deadlocks with filesystem freeze operations. This change was made by commit ce8ea7cc6eb313 ("btrfs: don't call btrfs_start_delalloc_roots in flushoncommit"). After that change we started producing that warning, and every now and then a user reports this since the warning happens too often, it spams dmesg/syslog, and a user is unsure if this reflects any problem that might compromise the filesystem's reliability. We can not just lock the sb->s_umount semaphore before calling writeback_inodes_sb(), because that would at least deadlock with filesystem freezing, since at fs/super.c:freeze_super() sync_filesystem() is called while we are holding that semaphore in write mode, and that can trigger a transaction commit, resulting in a deadlock. It would also trigger the same type of deadlock in the unmount path. Possibly, it could also introduce some other locking dependencies that lockdep would report. To fix this call try_to_writeback_inodes_sb() instead of writeback_inodes_sb(), because that will try to read lock sb->s_umount and then will only call writeback_inodes_sb() if it was able to lock it. This is fine because the cases where it can't read lock sb->s_umount are during a filesystem unmount or during a filesystem freeze - in those cases sb->s_umount is write locked and sync_filesystem() is called, which calls writeback_inodes_sb(). In other words, in all cases where we can't take a read lock on sb->s_umount, writeback is already being triggered elsewhere. An alternative would be to call btrfs_start_delalloc_roots() with a number of pages different from LONG_MAX, for example matching the number of delalloc bytes we currently have, in ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48918	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: mvm: check debugfs_dir ptr before use When "debugfs=off" is used on the kernel command line, iwiwifi's mvm module uses an invalid/unchecked debugfs_dir pointer and causes a BUG: BUG: kernel NULL pointer dereference, address: 000000000000004f #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP CPU: 1 PID: 503 Comm: modprobe Tainted: G W 5.17.0-rc5 #7 Hardware name: Dell Inc. Inspiron 15 5510/076F7Y, BIOS 2.4.1 11/05/2021 RIP: 0010:iwl_mvm_dbgfs_register+0x692/0x700 [iwlmvm] Code: 69 a0 be 80 01 00 00 48 c7 c7 50 73 6a a0 e8 95 cf ee e0 48 8b 83 b0 1e 00 00 48 c7 c2 54 73 6a a0 be 64 00 00 00 48 8d 7d 8c <48> 8b 48 50 e8 15 22 07 e1 48 8b 43 28 48 8d 55 8c 48 c7 c7 5f 73 RSP: 0018:ffffc90000a0ba68 EFLAGS: 00010246 RAX: ffffffffffffffff RBX: ffff88817d6e3328 RCX: ffff88817d6e3328 RDX: ffffffffa06a7354 RSI: 0000000000000064 RDI: ffffc90000a0ba6c RBP: ffffc90000a0bae0 R08: ffffffff824e4880 R09: ffffffffa069d620 R10: ffffc90000a0ba00 R11: ffffffffffffffff R12: 0000000000000000 R13: ffffc90000a0bb28 R14: ffff88817d6e3328 R15: ffff88817d6e3320 FS: 00007f64dd92d740(0000) GS:ffff88847f640000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004f CR3: 000000016fc79001 CR4: 0000000000770ee0 PKRU: 55555554 Call Trace: <TASK> ? iwl_mvm_mac_setup_register+0xbdc/0xda0 [iwlmvm] iwl_mvm_start_post_nvm+0x71/0x100 [iwlmvm] iwl_op_mode_mvm_start+0xab8/0xb30 [iwlmvm] _iwl_op_mode_start+0x6f/0xd0 [iwlwifi] iwl_opmode_register+0x6a/0xe0 [iwlwifi] ? 0xffffffffa0231000 iwl_mvm_init+0x35/0x1000 [iwlmvm] ? 0xffffffffa0231000 do_one_initcall+0x5a/0x1b0 ? kmem_cache_alloc+0x1e5/0x2f0 ? do_init_module+0x1e/0x220 do_init_module+0x48/0x220 load_module+0x2602/0x2bc0 ? __kernel_read+0x145/0x2e0 ? kernel_read_file+0x229/0x290 __do_sys_finit_module+0xc5/0x130 ? __do_sys_finit_module+0xc5/0x130 __x64_sys_finit_module+0x13/0x20 do_syscall_64+0x38/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f64dda564dd Code: 5b 41 5c c3 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 1b 29 0f 00 f7 d8 64 89 01 48 RSP: 002b:00007ffdba393f88 EFLAGS: 00000246 ORIG_RAX: 0000000000000139 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f64dda564dd RDX: 0000000000000000 RSI: 00005575399e2ab2 RDI: 0000000000000001 RBP: 000055753a91c5e0 R08: 0000000000000000 R09: 0000000000000002 R10: 0000000000000001 R11: 0000000000000246 R12: 00005575399e2ab2 R13: 000055753a91ceb0 R14: 0000000000000000 R15: 000055753a923018 </TASK> Modules linked in: btintel(+) btmtk bluetooth vfat snd_hda_codec_hdmi fat snd_hda_codec_realtek snd_hda_codec_generic iwlmvm(+) snd_sof_pci_intel_tgl mac80211 snd_sof_intel_hda_common soundwire_intel soundwire_generic_allocation soundwire_cadence soundwire_bus snd_sof_intel_hda snd_sof_pci snd_sof snd_sof_xtensa_dsp snd_soc_hdac_hda snd_hda_ext_core snd_soc_acpi_intel_match snd_soc_acpi snd_soc_core btrfs snd_compress snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec raid6_pq iwlwifi snd_hda_core snd_pcm snd_timer snd soundcore cfg80211 intel_ish_ipc(+) thunderbolt rfkill intel_ishtp ucsi_acpi wmi i2c_hid_acpi i2c_hid evdev CR2: 000000000000004f ---[end trace 0000000000000000]--- Check the debugfs_dir pointer for an error before using it. [change to make both conditional]	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48901	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not start relocation until in progress drops are done We hit a bug with a recovering relocation on mount for one of our file systems in production. I reproduced this locally by injecting errors into snapshot delete with balance running at the same time. This presented as an error while looking up an extent item WARNING: CPU: 5 PID: 1501 at fs/btrfs/extent-tree.c:866 lookup_inline_extent_backref+0x647/0x680 CPU: 5 PID: 1501 Comm: btrfs-balance Not tainted 5.16.0-rc8+ #8 RIP: 0010:lookup_inline_extent_backref+0x647/0x680 RSP: 0018:ffffae0a023ab960 EFLAGS: 00010202 RAX: 0000000000000001 RBX: 0000000000000000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 000000000000000c RDI: 0000000000000000 RBP: ffff943fd2a39b60 R08: 0000000000000000 R09: 0000000000000001 R10: 0001434088152de0 R11: 0000000000000000 R12: 0000000001d05000 R13: ffff943fd2a39b60 R14: ffff943fdb96f2a0 R15: ffff9442fc923000 FS: 0000000000000000(0000) GS:ffff944e9eb40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f1157b1fca8 CR3: 000000010f092000 CR4: 0000000000350ee0 Call Trace: <TASK> insert_inline_extent_backref+0x46/0xd0 __btrfs_inc_extent_ref.isra.0+0x5f/0x200 ? btrfs_merge_delayed_refs+0x164/0x190 __btrfs_run_delayed_refs+0x561/0xfa0 ? btrfs_search_slot+0x7b4/0xb30 ? btrfs_update_root+0x1a9/0x2c0 btrfs_run_delayed_refs+0x73/0x1f0 ? btrfs_update_root+0x1a9/0x2c0 btrfs_commit_transaction+0x50/0xa50 ? btrfs_update_reloc_root+0x122/0x220 prepare_to_merge+0x29f/0x320 relocate_block_group+0x2b8/0x550 btrfs_relocate_block_group+0x1a6/0x350 btrfs_relocate_chunk+0x27/0xe0 btrfs_balance+0x777/0xe60 balance_kthread+0x35/0x50 ? btrfs_balance+0xe60/0xe60 kthread+0x16b/0x190 ? set_kthread_struct+0x40/0x40 ret_from_fork+0x22/0x30 </TASK> Normally snapshot deletion and relocation are excluded from running at the same time by the fs_info->cleaner_mutex. However if we had a pending balance waiting to get the ->cleaner_mutex, and a snapshot deletion was running, and then the box crashed, we would come up in a state where we have a half deleted snapshot. Again, in the normal case the snapshot deletion needs to complete before relocation can start, but in this case relocation could very well start before the snapshot deletion completes, as we simply add the root to the dead roots list and wait for the next time the cleaner runs to clean up the snapshot. Fix this by setting a bit on the fs_info if we have any DEAD_ROOT's that had a pending drop_progress key. If they do then we know we were in the middle of the drop operation and set a flag on the fs_info. Then balance can wait until this flag is cleared to start up again. If there are DEAD_ROOT's that don't have a drop_progress set then we're safe to start balance right away as we'll be properly protected by the cleaner_mutex.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48916	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix double list_add when enabling VMD in scalable mode When enabling VMD and IOMMU scalable mode, the following kernel panic call trace/kernel log is shown in Eagle Stream platform (Sapphire Rapids CPU) during booting: pci 0000:59:00.5: Adding to iommu group 42 ... vmd 0000:59:00.5: PCI host bridge to bus 10000:80 pci 10000:80:01.0: [8086:352a] type 01 class 0x060400 pci 10000:80:01.0: reg 0x10: [mem 0x00000000-0x0001ffff 64bit] pci 10000:80:01.0: enabling Extended Tags pci 10000:80:01.0: PME# supported from D0 D3hot D3cold pci 10000:80:01.0: DMAR: Setup RID2PASID failed pci 10000:80:01.0: Failed to add to iommu group 42: -16 pci 10000:80:03.0: [8086:352b] type 01 class 0x060400 pci 10000:80:03.0: reg 0x10: [mem 0x00000000-0x0001ffff 64bit] pci 10000:80:03.0: enabling Extended Tags pci 10000:80:03.0: PME# supported from D0 D3hot D3cold ------------[cut here]------------ kernel BUG at lib/list_debug.c:29! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 7 Comm: kworker/0:1 Not tainted 5.17.0-rc3+ #7 Hardware name: Lenovo ThinkSystem SR650V3/SB27A86647, BIOS ESE101Y-1.00 01/13/2022 Workqueue: events work_for_cpu_fn RIP: 0010:__list_add_valid.cold+0x26/0x3f Code: 9a 4a ab ff 4c 89 c1 48 c7 c7 40 0c d9 9e e8 b9 b1 fe ff 0f 0b 48 89 f2 4c 89 c1 48 89 fe 48 c7 c7 f0 0c d9 9e e8 a2 b1 fe ff <0f> 0b 48 89 d1 4c 89 c6 4c 89 ca 48 c7 c7 98 0c d9 9e e8 8b b1 fe RSP: 0000:ff5ad434865b3a40 EFLAGS: 00010246 RAX: 0000000000000058 RBX: ff4d61160b74b880 RCX: ff4d61255e1fffa8 RDX: 0000000000000000 RSI: 00000000fffeffff RDI: ffffffff9fd34f20 RBP: ff4d611d8e245c00 R08: 0000000000000000 R09: ff5ad434865b3888 R10: ff5ad434865b3880 R11: ff4d61257fdc6fe8 R12: ff4d61160b74b8a0 R13: ff4d61160b74b8a0 R14: ff4d611d8e245c10 R15: ff4d611d8001ba70 FS: 0000000000000000(0000) GS:ff4d611d5ea00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ff4d611fa1401000 CR3: 0000000aa0210001 CR4: 0000000000771ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe07f0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> intel_pasid_alloc_table+0x9c/0x1d0 dmar_insert_one_dev_info+0x423/0x540 ? device_to_iommu+0x12d/0x2f0 intel_iommu_attach_device+0x116/0x290 __iommu_attach_device+0x1a/0x90 iommu_group_add_device+0x190/0x2c0 __iommu_probe_device+0x13e/0x250 iommu_probe_device+0x24/0x150 iommu_bus_notifier+0x69/0x90 blocking_notifier_call_chain+0x5a/0x80 device_add+0x3db/0x7b0 ? arch_memremap_can_ram_remap+0x19/0x50 ? memremap+0x75/0x140 pci_device_add+0x193/0x1d0 pci_scan_single_device+0xb9/0xf0 pci_scan_slot+0x4c/0x110 pci_scan_child_bus_extend+0x3a/0x290 vmd_enable_domain.constprop.0+0x63e/0x820 vmd_probe+0x163/0x190 local_pci_probe+0x42/0x80 work_for_cpu_fn+0x13/0x20 process_one_work+0x1e2/0x3b0 worker_thread+0x1c4/0x3a0 ? rescuer_thread+0x370/0x370 kthread+0xc7/0xf0 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x1f/0x30 </TASK> Modules linked in: ---[end trace 0000000000000000]--- ... Kernel panic - not syncing: Fatal exception Kernel Offset: 0x1ca00000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff) ---[end Kernel panic - not syncing: Fatal exception]--- The following 'lspci' output shows devices '10000:80:*' are subdevices of the VMD device 0000:59:00.5: $ lspci ... 0000:59:00.5 RAID bus controller: Intel Corporation Volume Management Device NVMe RAID Controller (rev 20) ... 10000:80:01.0 PCI bridge: Intel Corporation Device 352a (rev 03) 10000:80:03.0 PCI bridge: Intel Corporation Device 352b (rev 03) 10000:80:05.0 PCI bridge: Intel Corporation Device 352c (rev 03) 10000:80:07.0 PCI bridge: Intel Corporation Device 352d (rev 03) 10000:81:00.0 Non-Volatile memory controller: Intel Corporation NVMe Datacenter SSD [3DNAND, Beta Rock Controller] 10000:82:00 ---truncated---	5.5	More Details
CVE-2022-48915	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Fix TZ_GET_TRIP NULL pointer dereference Do not call get_trip_hyst() from thermal_genl_cmd_tz_get_trip() if the thermal zone does not define one.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48914	In the Linux kernel, the following vulnerability has been resolved: xen/netfront: destroy queues before real_num_tx_queues is zeroed xennet_destroy_queues() relies on info->netdev->real_num_tx_queues to delete queues. Since d7dac083414eb5bb99a6d2ed53dc2c1b405224e5 ("net-sysfs: update the queue counts in the unregistration path"), unregister_netdev() indirectly sets real_num_tx_queues to 0. Those two facts together means, that xennet_destroy_queues() called from xennet_remove() cannot do its job, because it's called after unregister_netdev(). This results in kfree-ing queues that are still linked in napi, which ultimately crashes: BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 52 Comm: xenwatch Tainted: G W 5.16.10-1.32.fc32.qubes.x86_64+ #226 RIP: 0010:free_netdev+0xa3/0x1a0 Code: ff 48 89 df e8 2e e9 00 00 48 8b 43 50 48 8b 08 48 8d b8 a0 fe ff ff 48 8d a9 a0 fe ff ff 49 39 c4 75 26 eb 47 e8 ed c1 66 ff <48> 8b 85 60 01 00 00 48 8d 95 60 01 00 00 48 89 ef 48 2d 60 01 00 RSP: 0000:ffffc90000bcfd00 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffff88800edad000 RCX: 0000000000000000 RDX: 0000000000000001 RSI: ffffc90000bcfc30 RDI: 00000000ffffffff RBP: ffffffffffffffea0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000001 R12: ffff88800edad050 R13: ffff8880065f8f88 R14: 0000000000000000 R15: ffff8880066c6680 FS: 0000000000000000(0000) GS:ffff8880f3300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 00000000e998c006 CR4: 0000000003706e0 Call Trace: <TASK> xennet_remove+0x13d/0x300 [xen_netfront] xenbus_dev_remove+0x6d/0xf0 __device_release_driver+0x17a/0x240 device_release_driver+0x24/0x30 bus_remove_device+0xd8/0x140 device_del+0x18b/0x410 ? _raw_spin_unlock+0x16/0x30 ? klist_iter_exit+0x14/0x20 ? xenbus_dev_request_and_reply+0x80/0x80 device_unregister+0x13/0x60 xenbus_dev_changed+0x18e/0x1f0 xenwatch_thread+0xc0/0x1a0 ? do_wait_intr_irq+0xa0/0xa0 kthread+0x16b/0x190 ? set_kthread_struct+0x40/0x40 ret_from_fork+0x22/0x30 </TASK> Fix this by calling xennet_destroy_queues() from xennet_uninit(), when real_num_tx_queues is still available. This ensures that queues are destroyed when real_num_tx_queues is set to 0, regardless of how unregister_netdev() was called. Originally reported at https://github.com/QubesOS/qubes-issues/issues/7257	5.5	More Details
CVE-2022-48911	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_queue: fix possible use-after-free Eric Dumazet says: The sock_hold() side seems suspect, because there is no guarantee that sk_refcnt is not already 0. On failure, we cannot queue the packet and need to indicate an error. The packet will be dropped by the caller. v2: split skb prefetch hunk into separate change	5.5	More Details
CVE-2022-48910	In the Linux kernel, the following vulnerability has been resolved: net: ipv6: ensure we call ipv6_mc_down() at most once There are two reasons for addrconf_notify() to be called with NETDEV_DOWN: either the network device is actually going down, or IPv6 was disabled on the interface. If either of them stays down while the other is toggled, we repeatedly call the code for NETDEV_DOWN, including ipv6_mc_down(), while never calling the corresponding ipv6_mc_up() in between. This will cause a new entry in idev->mc_tomb to be allocated for each multicast group the interface is subscribed to, which in turn leaks one struct ifmcaddr6 per nontrivial multicast group the interface is subscribed to. The following reproducer will leak at least $n objects: ip addr add ff2e::4242/32 dev eth0 autojoin sysctl -w net.ipv6.conf.eth0.disable_ipv6=1 for i in $(seq 1 $n); do ip link set up eth0; ip link set down eth0 done Joining groups with IPV6_ADD_MEMBERSHIP (unprivileged) or setting the sysctl net.ipv6.conf.eth0.forwarding to 1 (=> subscribing to ff02::2) can also be used to create a nontrivial idev->mc_list, which will the leak objects with the right up-down-sequence. Based on both sources for NETDEV_DOWN events the interface IPv6 state should be considered: - not ready if the network interface is not ready OR IPv6 is disabled for it - ready if the network interface is ready AND IPv6 is enabled for it The functions ipv6_mc_up() and ipv6_down() should only be run when this state changes. Implement this by remembering when the IPv6 state is ready, and only run ipv6_mc_down() if it actually changed from ready to not ready. The other direction (not ready -> ready) already works correctly, as: - the interface notification triggered codepath for NETDEV_UP / NETDEV_CHANGE returns early if ipv6 is disabled, and - the disable_ipv6=0 triggered codepath skips fully initializing the interface as long as addrconf_link_ready(dev) returns false - calling ipv6_mc_up() repeatedly does not leak anything	5.5	More Details
CVE-2022-48909	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix connection leak There's a potential leak issue under following execution sequence : smc_release smc_connect_work if (sk->sk_state == SMC_INIT) send_clc_confirim tcp_abort(); ... sk.sk_state = SMC_ACTIVE smc_close_active switch(sk->sk_state) { ... case SMC_ACTIVE: smc_close_final() // then wait peer closed Unfortunately, tcp_abort() may discard CLC CONFIRM messages that are still in the tcp send buffer, in which case our connection token cannot be delivered to the server side, which means that we cannot get a passive close message at all. Therefore, it is impossible for the to be disconnected at all. This patch tries a very simple way to avoid this issue, once the state has changed to SMC_ACTIVE after tcp_abort(), we can actively abort the smc connection, considering that the state is SMC_INIT before tcp_abort(), abandoning the complete disconnection process should not cause too much problem. In fact, this problem may exist as long as the CLC CONFIRM message is not received by the server. Whether a timer should be added after smc_close_final() needs to be discussed in the future. But even so, this patch provides a faster release for connection in above case, it should also be valuable.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48902	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not WARN_ON() if we have PageError set Whenever we do any extent buffer operations we call assert_eb_page_uptodate() to complain loudly if we're operating on an non-uptodate page. Our overnight tests caught this warning earlier this week WARNING: CPU: 1 PID: 553508 at fs/btrfs/extent_io.c:6849 assert_eb_page_uptodate+0x3f/0x50 CPU: 1 PID: 553508 Comm: kworker/u4:13 Tainted: G W 5.17.0-rc3+ #564 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.13.0-2.fc32 04/01/2014 Workqueue: btrfs-cache btrfs_work_helper RIP: 0010:assert_eb_page_uptodate+0x3f/0x50 RSP: 0018:ffffa961440a7c68 EFLAGS: 00010246 RAX: 0017ffffc0002112 RBX: ffffe6e74453f9c0 RCX: 0000000000001000 RDX: ffffe6e74467c887 RSI: ffffe6e74453f9c0 RDI: ffff8d4c5efc2fc0 RBP: 0000000000000d56 R08: ffff8d4d4a224000 R09: 0000000000000000 R10: 00015817fa9d1ef0 R11: 000000000000000c R12: 00000000000007b1 R13: ffff8d4c5efc2fc0 R14: 0000000001500000 R15: 0000000001cb1000 FS: 0000000000000000(0000) GS:ffff8d4dbbd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ff31d3448d8 CR3: 0000000118be8004 CR4: 0000000000370ee0 Call Trace: extent_buffer_test_bit+0x3f/0x70 free_space_test_bit+0xa6/0xc0 load_free_space_tree+0x1f6/0x470 caching_thread+0x454/0x630 ? rcu_read_lock_sched_held+0x12/0x60 ? rcu_read_lock_sched_held+0x12/0x60 ? rcu_read_lock_sched_held+0x12/0x60 ? lock_release+0x1f0/0x2d0 btrfs_work_helper+0xf2/0x3e0 ? lock_release+0x1f0/0x2d0 ? finish_task_switch.isra.0+0xf9/0x3a0 process_one_work+0x26d/0x580 ? process_one_work+0x580/0x580 worker_thread+0x55/0x3b0 ? process_one_work+0x580/0x580 kthread+0xf0/0x120 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x1f/0x30 This was partially fixed by c2e39305299f01 ("btrfs: clear extent buffer uptodate when we fail to write it"), however all that fix did was keep us from finding extent buffers after a failed writeout. It didn't keep us from continuing to use a buffer that we already had found. In this case we're searching the commit root to cache the block group, so we can start committing the transaction and switch the commit root and then start writing. After the switch we can look up an extent buffer that hasn't been written yet and start processing that block group. Then we fail to write that block out and clear Uptodate on the page, and then we start spewing these errors. Normally we're protected by the tree lock to a certain degree here. If we read a block we have that block read locked, and we block the writer from locking the block before we submit it for the write. However this isn't necessarily fool proof because the read could happen before we do the submit_bio and after we locked and unlocked the extent buffer. Also in this particular case we have path->skip_locking set, so that won't save us here. We'll simply get a block that was valid when we read it, but became invalid while we were using it. What we really want is to catch the case where we've "read" a block but it's not marked Uptodate. On read we ClearPageError(), so if we're !Uptodate and !Error we know we didn't do the right thing for reading the page. Fix this by checking !Uptodate && !Error, this way we will not complain if our buffer gets invalidated while we're using it, and we'll maintain the spirit of the check which is to make sure we have a fully in-cache block while we're messing with it.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48903	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix relocation crash due to premature return from btrfs_commit_transaction() We are seeing crashes similar to the following trace: [38.969182] WARNING: CPU: 20 PID: 2105 at fs/btrfs/relocation.c:4070 btrfs_relocate_block_group+0x2dc/0x340 [btrfs] [38.973556] CPU: 20 PID: 2105 Comm: btrfs Not tainted 5.17.0-rc4 #54 [38.974580] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.12.0-59-gc9ba5276e321-prebuilt.qemu.org 04/01/2014 [38.976539] RIP: 0010:btrfs_relocate_block_group+0x2dc/0x340 [btrfs] [38.980336] RSP: 0000:ffffb0dd42e03c20 EFLAGS: 00010206 [38.981218] RAX: ffff96cfc4ede800 RBX: ffff96cfc3ce0000 RCX: 000000000002ca14 [38.982560] RDX: 0000000000000000 RSI: 4cfd109a0bcb5d7f RDI: ffff96cfc3ce0360 [38.983619] RBP: ffff96cfc309c000 R08: 0000000000000000 R09: 0000000000000000 [38.984678] R10: ffff96cec0000001 R11: ffffe84c80000000 R12: ffff96cfc4ede800 [38.985735] R13: 0000000000000000 R14: 0000000000000000 R15: ffff96cfc3ce0360 [38.987146] FS: 00007f11c15218c0(0000) GS:ffff96d6dfb00000(0000) knlGS:0000000000000000 [38.988662] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [38.989398] CR2: 00007ffc922c8e60 CR3: 00000001147a6001 CR4: 0000000000370ee0 [38.990279] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [38.991219] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [38.992528] Call Trace: [38.992854] <TASK> [38.993148] btrfs_relocate_chunk+0x27/0xe0 [btrfs] [38.993941] btrfs_balance+0x78e/0xea0 [btrfs] [38.994801] ? vsnprintf+0x33c/0x520 [38.995368] ? __kmalloc_track_caller+0x351/0x440 [38.996198] btrfs_ioctl_balance+0x2b9/0x3a0 [btrfs] [38.997084] btrfs_ioctl+0x11b0/0x2da0 [btrfs] [38.997867] ? mod_objcg_state+0xee/0x340 [38.998552] ? seq_release+0x24/0x30 [38.999184] ? proc_nr_files+0x30/0x30 [38.999654] ? call_rcu+0xc8/0x2f0 [39.000228] ? __x64_sys_ioctl+0x84/0xc0 [39.000872] ? btrfs_ioctl_get_supported_features+0x30/0x30 [btrfs] [39.001973] __x64_sys_ioctl+0x84/0xc0 [39.002566] do_syscall_64+0x3a/0x80 [39.003011] entry_SYSCALL_64_after_hwframe+0x44/0xae [39.003735] RIP: 0033:0x7f11c166959b [39.007324] RSP: 002b:00007fff2543e998 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [39.008521] RAX: ffffffffffffffda RBX: 00007f11c1521698 RCX: 00007f11c166959b [39.009833] RDX: 00007fff2543ea40 RSI: 00000000c4009420 RDI: 0000000000000003 [39.011270] RBP: 0000000000000003 R08: 0000000000000013 R09: 00007f11c16f94e0 [39.012581] R10: 0000000000000000 R11: 0000000000000246 R12: 00007fff25440df3 [39.014046] R13: 0000000000000000 R14: 00007fff2543ea40 R15: 0000000000000001 [39.015040] </TASK> [39.015418] ---[end trace 0000000000000000]--- [43.131559] ------------[cut here]------------ [43.132234] kernel BUG at fs/btrfs/extent-tree.c:2717! [43.133031] invalid opcode: 0000 [#1] PREEMPT SMP PTI [43.133702] CPU: 1 PID: 1839 Comm: btrfs Tainted: G W 5.17.0-rc4 #54 [43.134863] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.12.0-59-gc9ba5276e321-prebuilt.qemu.org 04/01/2014 [43.136426] RIP: 0010:unpin_extent_range+0x37a/0x4f0 [btrfs] [43.139913] RSP: 0000:ffffb0dd4216bc70 EFLAGS: 00010246 [43.140629] RAX: 0000000000000000 RBX: ffff96cfc34490f8 RCX: 0000000000000001 [43.141604] RDX: 0000000080000001 RSI: 0000000051d00000 RDI: 00000000ffffffff [43.142645] RBP: 0000000000000000 R08: 0000000000000000 R09: ffff96cfd07dca50 [43.143669] R10: ffff96cfc46e8a00 R11: ffffffffffec000 R12: 0000000041d00000 [43.144657] R13: ffff96cfc3ce0000 R14: ffffb0dd4216bd08 R15: 0000000000000000 [43.145686] FS: 00007f7657dd68c0(0000) GS:ffff96d6df640000(0000) knlGS:0000000000000000 [43.146808] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [43.147584] CR2: 00007f7fe81bf5b0 CR3: 00000001093ee004 CR4: 0000000000370ee0 [43.148589] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [43.149581] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 00000000000 --- truncated---	5.5	More Details
CVE-2022-48908	In the Linux kernel, the following vulnerability has been resolved: net: arcnet: com20020: Fix null-ptr-deref in com20020pci_probe() During driver initialization, the pointer of card info, i.e. the variable 'ci' is required. However, the definition of 'com20020pci_id_table' reveals that this field is empty for some devices, which will cause null pointer dereference when initializing these devices. The following log reveals it: [3.973806] KASAN: null-ptr-deref in range [0x0000000000000028-0x000000000000002f] [3.973819] RIP: 0010:com20020pci_probe+0x18d/0x13e0 [com20020_pci] [3.975181] Call Trace: [3.976208] local_pci_probe+0x13f/0x210 [3.977248] pci_device_probe+0x34c/0x6d0 [3.977255] ? pci_uevent+0x470/0x470 [3.978265] really_probe+0x24c/0x8d0 [3.978273] __driver_probe_device+0x1b3/0x280 [3.979288] driver_probe_device+0x50/0x370 Fix this by checking whether the 'ci' is a null pointer first.	5.5	More Details
CVE-2022-48907	In the Linux kernel, the following vulnerability has been resolved: auxdisplay: lcd2s: Fix memory leak in ->remove() Once allocated the struct lcd2s_data is never freed. Fix the memory leak by switching to devm_kzalloc().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48906	In the Linux kernel, the following vulnerability has been resolved: mptcp: Correctly set DATA_FIN timeout when number of retransmits is large Syzkaller with UBSAN uncovered a scenario where a large number of DATA_FIN retransmits caused a shift-out-of-bounds in the DATA_FIN timeout calculation: == UBSAN: shift-out-of-bounds in net/mptcp/protocol.c:470:29 shift exponent 32 is too large for 32-bit type 'unsigned int' CPU: 1 PID: 13059 Comm: kworker/1:0 Not tainted 5.17.0-rc2-00630-g5fbf21c90c60 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 Workqueue: events mptcp_worker Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 ubsan_epilogue+0xb/0x5a lib/ubsan.c:151 __ubsan_handle_shift_out_of_bounds.cold+0xb2/0x20e lib/ubsan.c:330 mptcp_set_datafin_timeout net/mptcp/protocol.c:470 [inline] __mptcp_retrans.cold+0x72/0x77 net/mptcp/protocol.c:2445 mptcp_worker+0x58a/0xa70 net/mptcp/protocol.c:2528 process_one_work+0x9df/0x16d0 kernel/workqueue.c:2307 worker_thread+0x95/0xe10 kernel/workqueue.c:2454 kthread+0x2f4/0x3b0 kernel/kthread.c:377 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK> == This change limits the maximum timeout by limiting the size of the shift, which keeps all intermediate values in-bounds.	5.5	More Details
CVE-2022-48904	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Fix I/O page table memory leak The current logic updates the I/O page table mode for the domain before calling the logic to free memory used for the page table. This results in IOMMU page table memory leak, and can be observed when launching VM w/ pass-through devices. Fix by freeing the memory used for page table before updating the mode.	5.5	More Details
CVE-2022-48905	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: free reset-work-item when flushing Fix a tiny memory leak when flushing the reset work queue.	5.5	More Details
CVE-2022-48923	In the Linux kernel, the following vulnerability has been resolved: btrfs: prevent copying too big compressed lzo segment Compressed length can be corrupted to be a lot larger than memory we have allocated for buffer. This will cause memcpy in copy_compressed_segment to write outside of allocated memory. This mostly results in stuck read syscall but sometimes when using btrfs send can get #GP kernel: general protection fault, probably for non-canonical address 0x841551d5c1000: 0000 [#1] PREEMPT SMP NOPTI kernel: CPU: 17 PID: 264 Comm: kworker/u256:7 Tainted: P OE 5.17.0-rc2-1 #12 kernel: Workqueue: btrfs-endio btrfs_work_helper [btrfs] kernel: RIP: 0010:lzo_decompress_bio (./include/linux/fortify-string.h:225 fs/btrfs/lzo.c:322 fs/btrfs/lzo.c:394) btrfs Code starting with the faulting instruction ========== 0:* 48 8b 06 mov (%rsi),%rax <-- trapping instruction 3: 48 8d 79 08 lea 0x8(%rcx),%rdi 7: 48 83 e7 f8 and $0xfffffffffffffff8,%rdi b: 48 89 01 mov %rax,(%rcx) e: 44 89 f0 mov %r14d,%eax 11: 48 8b 54 06 f8 mov -0x8(%rsi,%rax,1),%rdx kernel: RSP: 0018:ffffb110812efd50 EFLAGS: 00010212 kernel: RAX: 0000000000001000 RBX: 000000009ca264c8 RCX: ffff98996e6d8ff8 kernel: RDX: 0000000000000064 RSI: 000841551d5c1000 RDI: ffffffff9500435d kernel: RBP: ffff989a3be856c0 R08: 0000000000000000 R09: 0000000000000000 kernel: R10: 0000000000000000 R11: 0000000000001000 R12: ffff98996e6d8000 kernel: R13: 0000000000000008 R14: 0000000000001000 R15: 000841551d5c1000 kernel: FS: 0000000000000000(0000) GS:ffff98a09d640000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 00001e9f984d9ea8 CR3: 000000014971a000 CR4: 00000000003506e0 kernel: Call Trace: kernel: <TASK> kernel: end_compressed_bio_read (fs/btrfs/compression.c:104 fs/btrfs/compression.c:1363 fs/btrfs/compression.c:323) btrfs kernel: end_workqueue_fn (fs/btrfs/disk-io.c:1923) btrfs kernel: btrfs_work_helper (fs/btrfs/async-thread.c:326) btrfs kernel: process_one_work (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:212 ./include/trace/events/workqueue.h:108 kernel/workqueue.c:2312) kernel: worker_thread (./include/linux/list.h:292 kernel/workqueue.c:2455) kernel: ? process_one_work (kernel/workqueue.c:2397) kernel: kthread (kernel/kthread.c:377) kernel: ? kthread_complete_and_exit (kernel/kthread.c:332) kernel: ret_from_fork (arch/x86/entry/entry_64.S:301) kernel: </TASK>	5.5	More Details
CVE-2022-48917	In the Linux kernel, the following vulnerability has been resolved: ASoC: ops: Shift tested values in snd_soc_put_volsw() by +min While the $val/$val2 values passed in from userspace are always >= 0 integers, the limits of the control can be signed integers and the $min can be non-zero and less than zero. To correctly validate $val/$val2 against platform_max, add the $min offset to val first.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4441	In the Linux kernel, the following vulnerability has been resolved: spi: spi-zynq-qspi: Fix a NULL pointer dereference in zynq_qspi_exec_mem_op() In zynq_qspi_exec_mem_op(), kzalloc() is directly used in memset(), which could lead to a NULL pointer dereference on failure of kzalloc(). Fix this bug by adding a check of tmpbuf. This bug was found by a static analyzer. The analysis employs differential checking to identify inconsistent security operations (e.g., checks or kfrees) between two code paths and confirms that the inconsistent operations are not recovered in the current function or the callers, so they constitute bugs. Note that, as a bug found by static analysis, it can be a false positive or hard to trigger. Multiple researchers have cross-reviewed the bug. Builds with CONFIG_SPI_ZYNQ_QSPI=m show no new warnings, and our static analyzer no longer warns about this code.	5.5	More Details
CVE-2022-48938	In the Linux kernel, the following vulnerability has been resolved: CDC-NCM: avoid overflow in sanity checking A broken device may give an extreme offset like 0xFFF0 and a reasonable length for a fragment. In the sanity check as formulated now, this will create an integer overflow, defeating the sanity check. Both offset and offset + len need to be checked in such a manner that no overflow can occur. And those quantities should be unsigned.	5.5	More Details
CVE-2022-48929	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to out of bounds access into reg2btf_ids. When commit e6ac2450d6de ("bpf: Support bpf program calling kernel function") added kfunc support, it defined reg2btf_ids as a cheap way to translate the verifier reg type to the appropriate btf_vmlinux BTF ID, however commit c25b2ae13603 ("bpf: Replace PTR_TO_XXX_OR_NULL with PTR_TO_XXX | PTR_MAYBE_NULL") moved the __BPF_REG_TYPE_MAX from the last member of bpf_reg_type enum to after the base register types, and defined other variants using type flag composition. However, now, the direct usage of reg->type to index into reg2btf_ids may no longer fall into __BPF_REG_TYPE_MAX range, and hence lead to out of bounds access and kernel crash on dereference of bad pointer.	5.5	More Details
CVE-2022-48930	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync()	5.5	More Details
CVE-2022-48942	In the Linux kernel, the following vulnerability has been resolved: hwmon: Handle failure to register sensor with thermal zone correctly If an attempt is made to a sensor with a thermal zone and it fails, the call to devm_thermal_zone_of_sensor_register() may return -ENODEV. This may result in crashes similar to the following. Unable to handle kernel NULL pointer dereference at virtual address 00000000000003cd ... Internal error: Oops: 96000021 [#1] PREEMPT SMP ... pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mutex_lock+0x18/0x60 lr : thermal_zone_device_update+0x40/0x2e0 sp : ffff800014c4fc60 x29: ffff800014c4fc60 x28: ffff365ee3f6e000 x27: ffffdde218426790 x26: ffff365ee3f6e000 x25: 0000000000000000 x24: ffff365ee3f6e000 x23: ffffdde218426870 x22: ffff365ee3f6e000 x21: 00000000000003cd x20: ffff365ee8bf3308 x19: fffffffffffffed x18: 0000000000000000 x17: ffffdde21842689c x16: ffffdde1cb7a0b7c x15: 0000000000000040 x14: ffffdde21a4889a0 x13: 0000000000000228 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000000001120000 x7 : 0000000000000001 x6 : 0000000000000000 x5 : 0068000878e20f07 x4 : 0000000000000000 x3 : 00000000000003cd x2 : ffff365ee3f6e000 x1 : 0000000000000000 x0 : 00000000000003cd Call trace: mutex_lock+0x18/0x60 hwmon_notify_event+0xfc/0x110 0xffffdde1cb7a0a90 0xffffdde1cb7a0b7c irq_thread_fn+0x2c/0xa0 irq_thread+0x134/0x240 kthread+0x178/0x190 ret_from_fork+0x10/0x20 Code: d503201f d503201f d2800001 aa0103e4 (c8e47c02) Jon Hunter reports that the exact call sequence is: hwmon_notify_event() --> hwmon_thermal_notify() --> thermal_zone_device_update() --> update_temperature() --> mutex_lock() The hwmon core needs to handle all errors returned from calls to devm_thermal_zone_of_sensor_register(). If the call fails with -ENODEV, report that the sensor was not attached to a thermal zone but continue to register the hwmon device.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48940	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to incorrect copy_map_value When both bpf_spin_lock and bpf_timer are present in a BPF map value, copy_map_value needs to skirt both objects when copying a value into and out of the map. However, the current code does not set both s_off and t_off in copy_map_value, which leads to a crash when e.g. bpf_spin_lock is placed in map value with bpf_timer, as bpf_map_update_elem call will be able to overwrite the other timer object. When the issue is not fixed, an overwriting can produce the following splat: [root@(none) bpf]# ./test_progs -t timer_crash [15.930339] bpf_testmod: loading out-of-tree module taints kernel. [16.037849] == [16.038458] BUG: KASAN: user-memory-access in __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.038944] Write of size 8 at addr 0000000000043ec0 by task test_progs/325 [16.039399] [16.039514] CPU: 0 PID: 325 Comm: test_progs Tainted: G OE 5.16.0+ #278 [16.039983] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ArchLinux 1.15.0-1 04/01/2014 [16.040485] Call Trace: [16.040645] <TASK> [16.040805] dump_stack_lvl+0x59/0x73 [16.041069] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.041427] kasan_report.cold+0x116/0x11b [16.041673] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042040] __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042328] ? memcpy+0x39/0x60 [16.042552] ? pv_hash+0xd0/0xd0 [16.042785] ? lockdep_hardirqs_off+0x95/0xd0 [16.043079] __bpf_spin_lock_irqsave+0xdf/0xf0 [16.043366] ? bpf_get_current_comm+0x50/0x50 [16.043608] ? jhash+0x11a/0x270 [16.043848] bpf_timer_cancel+0x34/0xe0 [16.044119] bpf_prog_c4ea1c0f7449940d_sys_enter+0x7c/0x81 [16.044500] bpf_trampoline_6442477838_0+0x36/0x1000 [16.044836] __x64_sys_nanosleep+0x5/0x140 [16.045119] do_syscall_64+0x59/0x80 [16.045377] ? lock_is_held_type+0xe4/0x140 [16.045670] ? irqentry_exit_to_user_mode+0xa/0x40 [16.046001] ? mark_held_locks+0x24/0x90 [16.046287] ? asm_exc_page_fault+0x1e/0x30 [16.046569] ? asm_exc_page_fault+0x8/0x30 [16.046851] ? lockdep_hardirqs_on+0x7e/0x100 [16.047137] entry_SYSCALL_64_after_hwframe+0x44/0xae [16.047405] RIP: 0033:0x7f9e4831718d [16.047602] Code: b4 0c 00 0f 05 eb a9 66 0f 1f 44 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d b3 6c 0c 00 f7 d8 64 89 01 48 [16.048764] RSP: 002b:00007fff488086b8 EFLAGS: 00000206 ORIG_RAX: 0000000000000023 [16.049275] RAX: ffffffffffffffda RBX: 00007f9e48683740 RCX: 00007f9e4831718d [16.049747] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 00007fff488086d0 [16.050225] RBP: 00007fff488086f0 R08: 00007fff488085d7 R09: 00007f9e4cb594a0 [16.050648] R10: 0000000000000000 R11: 0000000000000206 R12: 00007f9e484cde30 [16.051124] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [16.051608] </TASK> [16.051762] ==	5.5	More Details
CVE-2022-48928	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function.	5.5	More Details
CVE-2022-48932	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: DR, Fix slab-out-of-bounds in mlx5_cmd_dr_create_fte When adding a rule with 32 destinations, we hit the following out-of-band access issue: BUG: KASAN: slab-out-of-bounds in mlx5_cmd_dr_create_fte+0x18ee/0x1e70 This patch fixes the issue by both increasing the allocated buffers to accommodate for the needed actions and by checking the number of actions to prevent this issue when a rule with too many actions is provided.	5.5	More Details
CVE-2022-48933	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix memory leak during stateful obj update stateful objects can be updated from the control plane. The transaction logic allocates a temporary object for this purpose. The ->init function was called for this object, so plain kfree() leaks resources. We must call ->destroy function of the object. nft_obj_destroy does this, but it also decrements the module refcount, but the update path doesn't increment it. To avoid special-casing the update object release, do module_get for the update case too and release it via nft_obj_destroy().	5.5	More Details
CVE-2022-48934	In the Linux kernel, the following vulnerability has been resolved: nfp: flower: Fix a potential leak in nfp_tunnel_add_shared_mac() ida_simple_get() returns an id between min (0) and max (NFP_MAX_MAC_INDEX) inclusive. So NFP_MAX_MAC_INDEX (0xff) is a valid id. In order for the error handling path to work correctly, the 'invalid' value for 'ida_idx' should not be in the 0..NFP_MAX_MAC_INDEX range, inclusive. So set it to -1.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48935	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via nf_tables_flowtable_destroy() otherwise hook core reports UAF. BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438 by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #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 lib/dump_stack.c:88 [inline] lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:106 lib/dump_stack.c:106 print_address_description+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247 __kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0 net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hook+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571 nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232 net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetlink.c:652 net/netfilter/nfnetlink.c:652 __nft_release_hook() calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free() which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds the flow_block.	5.5	More Details
CVE-2024-43863	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix a deadlock in dma buf fence polling Introduce a version of the fence ops that on release doesn't remove the fence from the pending list, and thus doesn't require a lock to fix poll->fence wait->fence unref deadlocks. vmwgfx overwrites the wait callback to iterate over the list of all fences and update their status, to do that it holds a lock to prevent the list modifcations from other threads. The fence destroy callback both deletes the fence and removes it from the list of pending fences, for which it holds a lock. dma buf polling cb unrefs a fence after it's been signaled: so the poll calls the wait, which signals the fences, which are being destroyed. The destruction tries to acquire the lock on the pending fences list which it can never get because it's held by the wait from which it was called. Old bug, but not a lot of userspace apps were using dma-buf polling interfaces. Fix those, in particular this fixes KDE stalls/deadlock.	5.5	More Details
CVE-2024-41846	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-41847	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-41848	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-41844	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-41875	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-42763	A Reflected Cross Site Scripting (XSS) vulnerability was found in the "/schedule.php" page of the Kashipara Bus Ticket Reservation System v1.0, which allows remote attackers to execute arbitrary code via the "bookingdate" parameter.	5.4	More Details
CVE-2024-39628	Cross-Site Request Forgery (CSRF) vulnerability in Saturday Drive Ninja Forms allows Cross Site Request Forgery.This issue affects Ninja Forms: from n/a through 3.8.6.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41876	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-41845	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-42762	A Stored Cross Site Scripting (XSS) vulnerability was found in "/history.php" in Kashipara Bus Ticket Reservation System v1.0, which allows remote attackers to execute arbitrary code via the Name, Phone, and Email parameter fields.	5.4	More Details
CVE-2024-43339	Cross-Site Request Forgery (CSRF) vulnerability in WebinarPress allows Cross-Site Scripting (XSS).This issue affects WebinarPress: from n/a through 1.33.20.	5.4	More Details
CVE-2024-41843	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-39645	Cross-Site Request Forgery (CSRF) vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a through 2.7.2.	5.4	More Details
CVE-2024-42790	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/music/index.php?page=test" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via the "page" parameter.	5.4	More Details
CVE-2024-8113	Stored XSS in organizer and event settings of pretix up to 2024.7.0 allows malicious event organizers to inject HTML tags into e-mail previews on settings page. The default Content Security Policy of pretix prevents execution of attacker-provided scripts, making exploitation unlikely. However, combined with a CSP bypass (which is not currently known) the vulnerability could be used to impersonate other organizers or staff users.	5.4	More Details
CVE-2024-43299	Cross-Site Request Forgery (CSRF) vulnerability in Softaculous Team SpeedyCache.This issue affects SpeedyCache: from n/a through 1.1.8.	5.4	More Details
CVE-2024-42766	Kashipara Bus Ticket Reservation System v1.0 0 is vulnerable to Incorrect Access Control via /deleteTicket.php.	5.4	More Details
CVE-2024-41878	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link.	5.4	More Details
CVE-2024-8163	A vulnerability classified as critical was found in Chengdu Everbrite Network Technology BeikeShop up to 1.5.5. Affected by this vulnerability is the function destroyFiles of the file /admin/file_manager/files. The manipulation of the argument files leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2024-41877	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-41841	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-8216	A vulnerability, which was classified as critical, has been found in nafisulbari/itsourcecode Insurance Management System 1.0. Affected by this issue is some unknown functionality of the file editPayment.php of the component Payment Handler. The manipulation of the argument recipt_no leads to improper access controls. The attack may be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42939	A cross-site scripting (XSS) vulnerability in the component /index/index.html of YZNCMS v1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the configured remarks text field.	5.4	More Details
CVE-2024-42918	itsourcecode Online Accreditation Management System contains a Cross Site Scripting vulnerability, which allows an attacker to execute arbitrary code via a crafted payload to the SCHOOLNAME, EMAILADDRES, CONTACTNO, COMPANYNAME and COMPANYCONTACTNO parameters in controller.php.	5.4	More Details
CVE-2024-36441	Swissphone DiCal-RED 4009 devices allow an unauthenticated attacker use a port-2101 TCP connection to gain access to operation messages that are received by the device.	5.4	More Details
CVE-2024-42550	A cross-site scripting (XSS) vulnerability in the component /email/welcome.php of Mini Inventory and Sales Management System commit 18aa3d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title parameter.	5.4	More Details
CVE-2024-8072	Mage AI allows remote unauthenticated attackers to leak the terminal server command history of arbitrary users	5.3	More Details
CVE-2024-43331	Missing Authorization vulnerability in VeronaLabs WP SMS.This issue affects WP SMS: from n/a through 6.9.3.	5.3	More Details
CVE-2024-6568	The Flamix: Bitrix24 and Contact Form 7 integrations plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.1.0. 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-2024-43259	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in JEM Plugins Order Export for WooCommerce.This issue affects Order Export for WooCommerce: from n/a through 3.23.	5.3	More Details
CVE-2024-43258	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Store Locator Plus.This issue affects Store Locator Plus: from n/a through 2311.17.01.	5.3	More Details
CVE-2024-45191	An issue was discovered in Matrix libolm through 3.2.16. The AES implementation is vulnerable to cache-timing attacks due to use of S-boxes. This is related to software that uses a lookup table for the SubWord step. This refers to the libolm implementation of Olm. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2023-48957	PureVPN Linux client 2.0.2-Productions fails to properly handle DNS queries, allowing them to bypass the VPN tunnel and be sent directly to the ISP or default DNS servers.	5.3	More Details
CVE-2024-42411	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to restrict the input in POST /api/v4/users which allows a user to manipulate the creation date in POST /api/v4/users tricking the admin into believing their account is much older.	5.3	More Details
CVE-2024-43264	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Mediavine Create by Mediavine.This issue affects Create by Mediavine: from n/a through 1.9.8.	5.3	More Details
CVE-2024-43283	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Contest Gallery.This issue affects Contest Gallery: from n/a through 23.1.2.	5.3	More Details
CVE-2024-43230	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Shared Files – File Upload Form Shared Files.This issue affects Shared Files: from n/a through 1.7.28.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7390	The WP Testimonial Widget plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnSaveTestimonailOrder function in all versions up to, and including, 3.0. This makes it possible for unauthenticated attackers to change the order of testimonials.	5.3	More Details
CVE-2024-43214	Missing Authorization vulnerability in myCred.This issue affects myCred: from n/a through 2.7.2.	5.3	More Details
CVE-2024-45244	Hyperledger Fabric through 2.5.9 does not verify that a request has a timestamp within the expected time window.	5.3	More Details
CVE-2024-45165	An issue was discovered in UCI IDOL 2 (aka uciIDOL or IDOL2) through 2.12. Data is sent between client and server with encryption. However, the key is derived from the string "(c)2007 UCI Software GmbH B.Boll" (without quotes). The key is both static and hardcoded. With access to messages, this results in message decryption and encryption by an attacker. Thus, it enables passive and active man-in-the-middle attacks.	5.3	More Details
CVE-2024-45192	An issue was discovered in Matrix libolm through 3.2.16. Cache-timing attacks can occur due to use of base64 when decoding group session keys. This refers to the libolm implementation of Olm. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2024-6499	The WordPress Button Plugin MaxButtons plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 9.7.8. 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-2024-41674	CKAN is an open-source data management system for powering data hubs and data portals. If there were connection issues with the Solr server, the internal Solr URL (potentially including credentials) could be leaked to package_search calls as part of the returned error message. This has been patched in CKAN 2.10.5 and 2.11.0.	5.3	More Details
CVE-2024-5288	An issue was discovered in wolfSSL before 5.7.0. A safe-error attack via Rowhammer, namely FAULT+PROBE, leads to ECDSA key disclosure. When WOLFSSL_CHECK_SIG_FAULTS is used in signing operations with private ECC keys, such as in server-side TLS connections, the connection is halted if any fault occurs. The success rate in a certain amount of connection requests can be processed via an advanced technique for ECDSA key recovery.	5.1	More Details
CVE-2024-6631	The ImageRecycle pdf & image compression plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several AJAX actions in all versions up to, and including, 3.1.14. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform unauthorized actions, such as updating plugin settings.	5.0	More Details
CVE-2024-43787	Hono is a Web application framework that provides support for any JavaScript runtime. Hono CSRF middleware can be bypassed using crafted Content-Type header. MIME types are case insensitive, but isRequestedByFormElementRe only matches lower-case. As a result, attacker can bypass csrf middleware using upper-case form-like MIME type. This vulnerability is fixed in 4.5.8.	5.0	More Details
CVE-2024-43443	Improper Neutralization of Input done by an attacker with admin privileges ('Cross-site Scripting') in Process Management modules of OTRS and ((OTRS)) Community Edition allows Cross-Site Scripting (XSS) within the Process Management targeting other admins. This issue affects: * OTRS from 7.0.X through 7.0.50 * OTRS 8.0.X * OTRS 2023.X * OTRS from 2024.X through 2024.5.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	4.9	More Details
CVE-2024-7634	NGINX Agent's "config_dirs" restriction feature allows a highly privileged attacker to gain the ability to write/overwrite files outside of the designated secure directory.	4.9	More Details
CVE-2024-43442	Improper Neutralization of Input done by an attacker with admin privileges ('Cross-site Scripting') in OTRS (System Configuration modules) and ((OTRS)) Community Edition allows Cross-Site Scripting (XSS) within the System Configuration targeting other admins. This issue affects: * OTRS from 7.0.X through 7.0.50 * OTRS 8.0.X * OTRS 2023.X * OTRS from 2024.X through 2024.5.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39810	Mattermost versions 9.5.x <= 9.5.7 and 9.10.x <= 9.10.0 fail to time limit and size limit the CA path file in the ElasticSearch configuration which allows a System Role with access to the Elasticsearch system console to add any file as a CA path field, such as /dev/zero and, after testing the connection, cause the application to crash.	4.9	More Details
CVE-2024-42771	A Stored Cross Site Scripting (XSS) vulnerability was found in " /admin/edit_room_controller.php" of the Kashipara Hotel Management System v1.0, which allows remote attackers to execute arbitrary code via "room_name" parameter.	4.8	More Details
CVE-2024-41842	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	4.8	More Details
CVE-2024-39836	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to ensure that remote/synthetic users cannot create sessions or reset passwords, which allows the munged email addresses, created by shared channels, to be used to receive email notifications and to reset passwords, when they are valid, functional emails.	4.8	More Details
CVE-2024-3282	The WP Table Builder WordPress plugin through 1.5.0 does not sanitise and escape some of its Table data, 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-2024-40111	A persistent (stored) cross-site scripting (XSS) vulnerability has been identified in Automad 2.0.0-alpha.4. This vulnerability enables an attacker to inject malicious JavaScript code into the template body. The injected code is stored within the flat file CMS and is executed in the browser of any user visiting the forum.	4.8	More Details
CVE-2022-39996	Cross Site Scripting vulnerability in Teldats Router RS123, RS123w allows attacker to execute arbitrary code via the cmdcookie parameter to the upgrade/query.php page.	4.8	More Details
CVE-2022-48941	In the Linux kernel, the following vulnerability has been resolved: ice: fix concurrent reset and removal of VFs Commit c503e63200c6 ("ice: Stop processing VF messages during teardown") introduced a driver state flag, ICE_VF_DEINIT_IN_PROGRESS, which is intended to prevent some issues with concurrently handling messages from VFs while tearing down the VFs. This change was motivated by crashes caused while tearing down and bringing up VFs in rapid succession. It turns out that the fix actually introduces issues with the VF driver caused because the PF no longer responds to any messages sent by the VF during its .remove routine. This results in the VF potentially removing its DMA memory before the PF has shut down the device queues. Additionally, the fix doesn't actually resolve concurrency issues within the ice driver. It is possible for a VF to initiate a reset just prior to the ice driver removing VFs. This can result in the remove task concurrently operating while the VF is being reset. This results in similar memory corruption and panics purportedly fixed by that commit. Fix this concurrency at its root by protecting both the reset and removal flows using the existing VF cfg_lock. This ensures that we cannot remove the VF while any outstanding critical tasks such as a virtchnl message or a reset are occurring. This locking change also fixes the root cause originally fixed by commit c503e63200c6 ("ice: Stop processing VF messages during teardown"), so we can simply revert it. Note that I kept these two changes together because simply reverting the original commit alone would leave the driver vulnerable to worse race conditions.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48898	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dp: do not complete dp_aux_cmd_fifo_tx() if irq is not for aux transfer There are 3 possible interrupt sources are handled by DP controller, HPDstatus, Controller state changes and Aux read/write transaction. At every irq, DP controller have to check isr status of every interrupt sources and service the interrupt if its isr status bits shows interrupts are pending. There is potential race condition may happen at current aux isr handler implementation since it is always complete dp_aux_cmd_fifo_tx() even irq is not for aux read or write transaction. This may cause aux read transaction return premature if host aux data read is in the middle of waiting for sink to complete transferring data to host while irq happen. This will cause host's receiving buffer contains unexpected data. This patch fixes this problem by checking aux isr and return immediately at aux isr handler if there are no any isr status bits set. Current there is a bug report regrading eDP edid corruption happen during system booting up. After lengthy debugging to found that VIDEO_READY interrupt was continuously firing during system booting up which cause dp_aux_isr() to complete dp_aux_cmd_fifo_tx() prematurely to retrieve data from aux hardware buffer which is not yet contains complete data transfer from sink. This cause edid corruption. Follows are the signature at kernel logs when problem happen, EDID has corrupt header panel-simple-dp-aux aux-aea0000.edp: Couldn't identify panel via EDID Changes in v2: -- do complete if (ret == IRQ_HANDLED) ay dp-aux_isr() -- add more commit text Changes in v3: -- add Stephen suggested -- dp_aux_isr() return IRQ_XXX back to caller -- dp_ctrl_isr() return IRQ_XXX back to caller Changes in v4: -- split into two patches Changes in v5: -- delete empty line between tags Changes in v6: -- remove extra "that" and fixed line more than 75 char at commit text Patchwork: https://patchwork.freedesktop.org/patch/516121/	4.7	More Details
CVE-2024-42770	A Stored Cross Site Scripting (XSS) vulnerability was found in "/core/signup_user.php" of Kashipara Hotel Management System v1.0, which allows remote attackers to execute arbitrary code via the "user_email" parameter.	4.7	More Details
CVE-2022-48899	In the Linux kernel, the following vulnerability has been resolved: drm/virtio: Fix GEM handle creation UAF Userspace can guess the handle value and try to race GEM object creation with handle close, resulting in a use-after-free if we dereference the object after dropping the handle's reference. For that reason, dropping the handle's reference must be done *after* we are done dereferencing the object.	4.7	More Details
CVE-2024-8166	A vulnerability has been found in Ruijie EG2000K 11.1(6)B2 and classified as critical. This vulnerability affects unknown code of the file /tool/index.php?c=download&a=save. The manipulation of the argument content leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-8120	The ImageRecycle pdf & image compression plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.14. This is due to missing or incorrect nonce validation on several functions in the class/class-image-otimizer.php file. This makes it possible for unauthenticated attackers to update plugin settings along with performing other actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.7	More Details
CVE-2022-48931	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B I delete list_head *C ----------|---------- configfs_unregister_subsystem I configfs_unregister_subsystem unlink_group I unlink_group unlink_obj I unlink_obj list_del_init I list_del_init __list_del_entry I __list_del_entry __list_del I __list_del // next == C I next->prev = prev I I next->prev = prev prev->next = next I I // prev == B I prev->next = next Fix this by adding mutex when calling link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root. So I create a mutex configfs_subsystem_mutex.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52896	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix race between quota rescan and disable leading to NULL pointer deref If we have one task trying to start the quota rescan worker while another one is trying to disable quotas, we can end up hitting a race that results in the quota rescan worker doing a NULL pointer dereference. The steps for this are the following: 1) Quotas are enabled; 2) Task A calls the quota rescan ioctl and enters btrfs_qgroup_rescan(). It calls qgroup_rescan_init() which returns 0 (success) and then joins a transaction and commits it; 3) Task B calls the quota disable ioctl and enters btrfs_quota_disable(). It clears the bit BTRFS_FS_QUOTA_ENABLED from fs_info->flags and calls btrfs_qgroup_wait_for_completion(), which returns immediately since the rescan worker is not yet running. Then it starts a transaction and locks fs_info->qgroup_ioctl_lock; 4) Task A queues the rescan worker, by calling btrfs_queue_work(); 5) The rescan worker starts, and calls rescan_should_stop() at the start of its while loop, which results in 0 iterations of the loop, since the flag BTRFS_FS_QUOTA_ENABLED was cleared from fs_info->flags by task B at step 3); 6) Task B sets fs_info->quota_root to NULL; 7) The rescan worker tries to start a transaction and uses fs_info->quota_root as the root argument for btrfs_start_transaction(). This results in a NULL pointer dereference down the call chain of btrfs_start_transaction(). The stack trace is something like the one reported in Link tag below: general protection fault, probably for non-canonical address 0xdffffc0000000041: 0000 [#1] PREEMPT SMP KASAN KASAN: null-ptr-deref in range [0x0000000000000208-0x000000000000020f] CPU: 1 PID: 34 Comm: kworker/u4:2 Not tainted 6.1.0-syzkaller-13872-gb6bb9676f216 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022 Workqueue: btrfs-qgroup-rescan btrfs_work_helper RIP: 0010:start_transaction+0x48/0x10f0 fs/btrfs/transaction.c:564 Code: 48 89 fb 48 (...) RSP: 0018:ffffc90000ab7ab0 EFLAGS: 00010206 RAX: 0000000000000041 RBX: 0000000000000208 RCX: ffff88801779ba80 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000000 RBP: dfffffc0000000000 R08: 0000000000000001 R09: fffff52000156f5d R10: fffff52000156f5d R11: 1ffff92000156f5c R12: 0000000000000000 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000003 FS: 0000000000000000(0000) GS:ffff8880b9900000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f2bea75b718 CR3: 000000001d0cc000 CR4: 00000000003506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> btrfs_qgroup_rescan_worker+0x3bb/0x6a0 fs/btrfs/qgroup.c:3402 btrfs_work_helper+0x312/0x850 fs/btrfs/async-thread.c:280 process_one_work+0x877/0xdb0 kernel/workqueue.c:2289 worker_thread+0xb14/0x1330 kernel/workqueue.c:2436 kthread+0x266/0x300 kernel/kthread.c:376 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:308 </TASK> Modules linked in: So fix this by having the rescan worker function not attempt to start a transaction if it didn't do any rescan work.	4.7	More Details
CVE-2023-52897	In the Linux kernel, the following vulnerability has been resolved: btrfs: qgroup: do not warn on record without old_roots populated [BUG] There are some reports from the mailing list that since v6.1 kernel, the WARN_ON() inside btrfs_qgroup_account_extent() gets triggered during rescan: WARNING: CPU: 3 PID: 6424 at fs/btrfs/qgroup.c:2756 btrfs_qgroup_account_extents+0x1ae/0x260 [btrfs] CPU: 3 PID: 6424 Comm: snapperd Tainted: P OE 6.1.2-1-default #1 openSUSE Tumbleweed 05c7a1b1b61d5627475528f71f50444637b5aad7 RIP: 0010:btrfs_qgroup_account_extents+0x1ae/0x260 [btrfs] Call Trace: <TASK> btrfs_commit_transaction+0x30c/0xb40 [btrfs c39c9c546c241c593f03bd6d5f39ea1b676250f6] ? start_transaction+0xc3/0x5b0 [btrfs c39c9c546c241c593f03bd6d5f39ea1b676250f6] btrfs_qgroup_rescan+0x42/0xc0 [btrfs c39c9c546c241c593f03bd6d5f39ea1b676250f6] btrfs_ioctl+0x1ab9/0x25c0 [btrfs c39c9c546c241c593f03bd6d5f39ea1b676250f6] ? __rseq_handle_notify_resume+0xa9/0x4a0 ? mntput_no_expire+0x4a/0x240 ? __seccomp_filter+0x319/0x4d0 __x64_sys_ioctl+0x90/0xd0 do_syscall_64+0x5b/0x80 ? syscall_exit_to_user_mode+0x17/0x40 ? do_syscall_64+0x67/0x80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7fd9b790d9bf </TASK> [CAUSE] Since commit e15e9f43c7ca ("btrfs: introduce BTRFS_QGROUP_RUNTIME_FLAG_NO_ACCOUNTING to skip qgroup accounting"), if our qgroup is already in inconsistent state, we will no longer do the time-consuming backref walk. This can leave some qgroup records without a valid old_roots ulist. Normally this is fine, as btrfs_qgroup_account_extents() would also skip those records if we have NO_ACCOUNTING flag set. But there is a small window, if we have NO_ACCOUNTING flag set, and inserted some qgroup_record without a old_roots ulist, but then the user triggered a qgroup rescan. During btrfs_qgroup_rescan(), we firstly clear NO_ACCOUNTING flag, then commit current transaction. And since we have a qgroup_record with old_roots = NULL, we trigger the WARN_ON() during btrfs_qgroup_account_extents(). [FIX] Unfortunately due to the introduction of NO_ACCOUNTING flag, the assumption that every qgroup_record would have its old_roots populated is no longer correct. Fix the false alerts and drop the WARN_ON().	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43892	In the Linux kernel, the following vulnerability has been resolved: memcg: protect concurrent access to mem_cgroup_idr Commit 73f576c04b94 ("mm: memcontrol: fix cgroup creation failure after many small jobs") decoupled the memcg IDs from the CSS ID space to fix the cgroup creation failures. It introduced IDR to maintain the memcg ID space. The IDR depends on external synchronization mechanisms for modifications. For the mem_cgroup_idr, the idr_alloc() and idr_replace() happen within css callback and thus are protected through cgroup_mutex from concurrent modifications. However idr_remove() for mem_cgroup_idr was not protected against concurrency and can be run concurrently for different memcgs when they hit their refcnt to zero. Fix that. We have been seeing list_lru based kernel crashes at a low frequency in our fleet for a long time. These crashes were in different part of list_lru code including list_lru_add(), list_lru_del() and reparenting code. Upon further inspection, it looked like for a given object (dentry and inode), the super_block's list_lru didn't have list_lru_one for the memcg of that object. The initial suspicions were either the object is not allocated through kmem_cache_alloc_lru() or somehow memcg_list_lru_alloc() failed to allocate list_lru_one() for a memcg but returned success. No evidence were found for these cases. Looking more deeply, we started seeing situations where valid memcg's id is not present in mem_cgroup_idr and in some cases multiple valid memcgs have same id and mem_cgroup_idr is pointing to one of them. So, the most reasonable explanation is that these situations can happen due to race between multiple idr_remove() calls or race between idr_alloc()/idr_replace() and idr_remove(). These races are causing multiple memcgs to acquire the same ID and then offlining of one of them would cleanup list_lrus on the system for all of them. Later access from other memcgs to the list_lru cause crashes due to missing list_lru_one.	4.7	More Details
CVE-2024-8150	A vulnerability was found in ContiNew Admin 3.2.0 and classified as critical. Affected by this issue is the function top.continew.starter.extension.crud.controller.BaseController#page of the file /api/system/user?deptId=1&page=1&size=10. The manipulation of the argument sort leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-43887	In the Linux kernel, the following vulnerability has been resolved: net/tcp: Disable TCP-AO static key after RCU grace period The lifetime of TCP-AO static_key is the same as the last tcp_ao_info. On the socket destruction tcp_ao_info ceases to be with RCU grace period, while tcp-ao static branch is currently deferred destructed. The static key definition is : DEFINE_STATIC_KEY_DEFERRED_FALSE(tcp_ao_needed, HZ); which means that if RCU grace period is delayed by more than a second and tcp_ao_needed is in the process of disablement, other CPUs may yet see tcp_ao_info which atent dead, but soon-to-be. And that breaks the assumption of static_key_fast_inc_not_disabled(). See the comment near the definition: > * The caller must make sure that the static key can't get disabled while > * in this function. It doesn't patch jump labels, only adds a user to > * an already enabled static key. Originally it was introduced in commit eb8c507296f6 ("jump_label: Prevent key->enabled int overflow"), which is needed for the atomic contexts, one of which would be the creation of a full socket from a request socket. In that atomic context, it's known by the presence of the key (md5/ao) that the static branch is already enabled. So, the ref counter for that static branch is just incremented instead of holding the proper mutex. static_key_fast_inc_not_disabled() is just a helper for such usage case. But it must not be used if the static branch could get disabled in parallel as it's not protected by jump_label_mutex and as a result, races with jump_label_update() implementation details. Happened on netdev test-bot[1], so not a theoretical issue: [] jump_label: Fatal kernel bug, unexpected op at tcp_inbound_hash+0x1a7/0x870 [ffffffffa8c4e9b7] (eb 50 0f 1f 44 != 66 90 0f 1f 00)) size:2 type:1 [] ------------[cut here]------------ [] kernel BUG at arch/x86/kernel/jump_label.c:73! [] Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN NOPTI [] CPU: 3 PID: 243 Comm: kworker/3:3 Not tainted 6.10.0-virtme #1 [] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [] Workqueue: events jump_label_update_timeout [] RIP: 0010:__jump_label_patch+0x2f6/0x350 ... [] Call Trace: [] <TASK> [] arch_jump_label_transform_queue+0x6c/0x110 [] __jump_label_update+0xef/0x350 [] __static_key_slow_dec_cpuslocked.part.0+0x3c/0x60 [] jump_label_update_timeout+0x2c/0x40 [] process_one_work+0xe3b/0x1670 [] worker_thread+0x587/0xce0 [] kthread+0x28a/0x350 [] ret_from_fork+0x31/0x70 [] ret_from_fork_asm+0x1a/0x30 [] </TASK> [] Modules linked in: veth [] ---[end trace 0000000000000000]--- [] RIP: 0010:__jump_label_patch+0x2f6/0x350 [1]: https://netdev-3.bots.linux.dev/vmksft-tcp-ao-dbg/results/696681/5-connect-deny-ipv6/stderr	4.7	More Details
CVE-2023-52898	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix null pointer dereference when host dies Make sure xhci_free_dev() and xhci_kill_endpoint_urbs() do not race and cause null pointer dereference when host suddenly dies. Usb core may call xhci_free_dev() which frees the xhci->devs[slot_id] virt device at the same time that xhci_kill_endpoint_urbs() tries to loop through all the device's endpoints, checking if there are any cancelled urbs left to give back. hold the xhci spinlock while freeing the virt device	4.7	More Details
CVE-2024-6879	The Quiz and Survey Master (QSM) WordPress plugin before 9.1.1 fails to validate and escape certain Quiz fields before displaying them on a page or post where the Quiz is embedded, which could allows contributor and above roles to perform Stored Cross-Site Scripting (XSS) attacks.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48869	In the Linux kernel, the following vulnerability has been resolved: USB: gadgetfs: Fix race between mounting and unmounting The syzbot fuzzer and Gerald Lee have identified a use-after-free bug in the gadgetfs driver, involving processes concurrently mounting and unmounting the gadgetfs filesystem. In particular, gadgetfs_fill_super() can race with gadgetfs_kill_sb(), causing the latter to deallocate the_device while the former is using it. The output from KASAN says, in part: BUG: KASAN: use-after-free in instrument_atomic_read_write include/linux/instrumented.h:102 [inline] BUG: KASAN: use-after-free in atomic_fetch_sub_release include/linux/atomic/atomic-instrumented.h:176 [inline] BUG: KASAN: use-after-free in __refcount_sub_and_test include/linux/refcount.h:272 [inline] BUG: KASAN: use-after-free in __refcount_dec_and_test include/linux/refcount.h:315 [inline] BUG: KASAN: use-after-free in refcount_dec_and_test include/linux/refcount.h:333 [inline] BUG: KASAN: use-after-free in put_dev drivers/usb/gadget/legacy/inode.c:159 [inline] BUG: KASAN: use-after-free in gadgetfs_kill_sb+0x33/0x100 drivers/usb/gadget/legacy/inode.c:2086 Write of size 4 at addr ffff8880276d7840 by task syz-executor126/18689 CPU: 0 PID: 18689 Comm: syz-executor126 Not tainted 6.1.0-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/26/2022 Call Trace: <TASK> ... atomic_fetch_sub_release include/linux/atomic/atomic-instrumented.h:176 [inline] __refcount_sub_and_test include/linux/refcount.h:272 [inline] __refcount_dec_and_test include/linux/refcount.h:315 [inline] refcount_dec_and_test include/linux/refcount.h:333 [inline] put_dev drivers/usb/gadget/legacy/inode.c:159 [inline] gadgetfs_kill_sb+0x33/0x100 drivers/usb/gadget/legacy/inode.c:2086 deactivate_locked_super+0xa7/0xf0 fs/super.c:332 vfs_get_super fs/super.c:1190 [inline] get_tree_single+0xd0/0x160 fs/super.c:1207 vfs_get_tree+0x88/0x270 fs/super.c:1531 vfs_fsconfig_locked fs/fsopen.c:232 [inline] The simplest solution is to ensure that gadgetfs_fill_super() and gadgetfs_kill_sb() are serialized by making them both acquire a new mutex.	4.7	More Details
CVE-2024-43891	In the Linux kernel, the following vulnerability has been resolved: tracing: Have format file honor EVENT_FILE_FL_FREED When eventfs was introduced, special care had to be done to coordinate the freeing of the file meta data with the files that are exposed to user space. The file meta data would have a ref count that is set when the file is created and would be decremented and freed after the last user that opened the file closed it. When the file meta data was to be freed, it would set a flag (EVENT_FILE_FL_FREED) to denote that the file is freed, and any new references made (like new opens or reads) would fail as it is marked freed. This allowed other meta data to be freed after this flag was set (under the event_mutex). All the files that were dynamically created in the events directory had a pointer to the file meta data and would call event_release() when the last reference to the user space file was closed. This would be the time that it is safe to free the file meta data. A shortcut was made for the "format" file. It's i_private would point to the "call" entry directly and not point to the file's meta data. This is because all format files are the same for the same "call", so it was thought there was no reason to differentiate them. The other files maintain state (like the "enable", "trigger", etc). But this meant if the file were to disappear, the "format" file would be unaware of it. This caused a race that could be trigger via the user_events test (that would create dynamic events and free them), and running a loop that would read the user_events format files: In one console run: # cd tools/testing/selftests/user_events # while true; do ./ftrace_test; done And in another console run: # cd /sys/kernel/tracing/ # while true; do cat events/user_events/__test_event/format; done 2>/dev/null With KASAN memory checking, it would trigger a use-after-free bug report (which was a real bug). This was because the format file was not checking the file's meta data flag "EVENT_FILE_FL_FREED", so it would access the event that the file meta data pointed to after the event was freed. After inspection, there are other locations that were found to not check the EVENT_FILE_FL_FREED flag when accessing the trace_event_file. Add a new helper function: event_file_file() that will make sure that the event_mutex is held, and will return NULL if the trace_event_file has the EVENT_FILE_FL_FREED flag set. Have the first reference of the struct file pointer use event_file_file() and check for NULL. Later uses can still use the event_file_data() helper function if the event_mutex is still held and was not released since the event_file_file() call.	4.7	More Details
CVE-2024-8071	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to restrict which roles can promote a user as system admin which allows a System Role with edit access to the permissions section of system console to update their role (e.g. member) to include the `manage_system` permission, effectively becoming a System Admin.	4.7	More Details
CVE-2024-8155	A vulnerability classified as critical was found in ContiNew Admin 3.2.0. Affected by this vulnerability is the function top.continew.starter.extension.crud.controller.BaseController#tree of the file /api/system/dept/tree?sort=parentId%2Casc&sort=sort%2Casc. The manipulation of the argument sort leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52909	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix handling of cached open files in nfsd4_open codepath Commit fb70bf124b05 ("NFSD: Instantiate a struct file when creating a regular NFSv4 file") added the ability to cache an open fd over a compound. There are a couple of problems with the way this currently works: It's racy, as a newly-created nfsd_file can end up with its PENDING bit cleared while the nf is hashed, and the nf_file pointer is still zeroed out. Other tasks can find it in this state and they expect to see a valid nf_file, and can oops if nf_file is NULL. Also, there is no guarantee that we'll end up creating a new nfsd_file if one is already in the hash. If an extant entry is in the hash with a valid nf_file, nfs4_get_vfs_file will clobber its nf_file pointer with the value of op_file and the old nf_file will leak. Fix both issues by making a new nfsd_file_acquirei_opened variant that takes an optional file pointer. If one is present when this is called, we'll take a new reference to it instead of trying to open the file. If the nfsd_file already has a valid nf_file, we'll just ignore the optional file and pass the nfsd_file back as-is. Also rework the tracepoints a bit to allow for an "opened" variant and don't try to avoid counting acquisitions in the case where we already have a cached open file.	4.7	More Details
CVE-2022-48921	In the Linux kernel, the following vulnerability has been resolved: sched/fair: Fix fault in reweight_entity Syzbot found a GPF in reweight_entity. This has been bisected to commit 4ef0c5c6b5ba ("kernel/sched: Fix sched_fork() access an invalid sched_task_group") There is a race between sched_post_fork() and setpriority(PRIO_PGRP) within a thread group that causes a null-ptr-deref in reweight_entity() in CFS. The scenario is that the main process spawns number of new threads, which then call setpriority(PRIO_PGRP, 0, -20), wait, and exit. For each of the new threads the copy_process() gets invoked, which adds the new task_struct and calls sched_post_fork() for it. In the above scenario there is a possibility that setpriority(PRIO_PGRP) and set_one_prio() will be called for a thread in the group that is just being created by copy_process(), and for which the sched_post_fork() has not been executed yet. This will trigger a null pointer dereference in reweight_entity(), as it will try to access the run queue pointer, which hasn't been set. Before the mentioned change the cfs_rq pointer for the task has been set in sched_fork(), which is called much earlier in copy_process(), before the new task is added to the thread_group. Now it is done in the sched_post_fork(), which is called after that. To fix the issue the remove the update_load param from the update_load param() function and call reweight_task() only if the task flag doesn't have the TASK_NEW flag set.	4.7	More Details
CVE-2024-40886	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to sanitize user inputs in the frontend that are used for redirection which allows for a one-click client-side path traversal that is leading to CSRF in User Management page of the system console.	4.6	More Details
CVE-2024-43790	Vim is an open source command line text editor. When performing a search and displaying the search-count message is disabled (:set shm+=S), the search pattern is displayed at the bottom of the screen in a buffer (msgbuf). When right-left mode (:set rl) is enabled, the search pattern is reversed. This happens by allocating a new buffer. If the search pattern contains some ASCII NUL characters, the buffer allocated will be smaller than the original allocated buffer (because for allocating the reversed buffer, the strlen() function is called, which only counts until it notices an ASCII NUL byte) and thus the original length indicator is wrong. This causes an overflow when accessing characters inside the msgbuf by the previously (now wrong) length of the msgbuf. The issue has been fixed as of Vim patch v9.1.0689.	4.5	More Details
CVE-2024-43371	CKAN is an open-source data management system for powering data hubs and data portals. There are a number of CKAN plugins, including XLoader, DataPusher, Resource proxy and ckanext-archiver, that work by downloading the contents of local or remote files in order to perform some actions with their contents (e.g. pushing to the DataStore, streaming contents or saving a local copy). All of them use the resource URL, and there are currently no checks to limit what URLs can be requested. This means that a malicious (or unaware) user can create a resource with a URL pointing to a place where they should not have access in order for one of the previous tools to retrieve it (known as a Server Side Request Forgery). Users wanting to protect against these kinds of attacks can use one or a combination of the following approaches: (1) Use a separate HTTP proxy like Squid that can be used to allow / disallow IPs, domains etc as needed, and make CKAN extensions aware of this setting via the ckan.download_proxy config option. (2) Implement custom firewall rules to prevent access to restricted resources. (3) Use custom validators on the resource url field to block/allow certain domains or IPs. All latest versions of the plugins listed above support the ckan.download_proxy settings. Support for this setting in the Resource Proxy plugin was included in CKAN 2.10.5 and 2.11.0.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43802	Vim is an improved version of the unix vi text editor. When flushing the typeahead buffer, Vim moves the current position in the typeahead buffer but does not check whether there is enough space left in the buffer to handle the next characters. So this may lead to the tb_off position within the typebuf variable to point outside of the valid buffer size, which can then later lead to a heap-buffer overflow in e.g. ins_typebuf(). Therefore, when flushing the typeahead buffer, check if there is enough space left before advancing the off position. If not, fall back to flush current typebuf contents. It's not quite clear yet, what can lead to this situation. It seems to happen when error messages occur (which will cause Vim to flush the typeahead buffer) in comnination with several long mappgins and so it may eventually move the off position out of a valid buffer size. Impact is low since it is not easily reproducible and requires to have several mappings active and run into some error condition. But when this happens, this will cause a crash. The issue has been fixed as of Vim patch v9.1.0697. Users are advised to upgrade. There are no known workarounds for this issue.	4.5	More Details
CVE-2023-0926	The Custom Permalinks plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.6.0 due to insufficient input sanitization and output escaping on tag names. This allows authenticated users, with editor-level permissions or greater to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, even when 'unfiltered_html' has been disabled.	4.4	More Details
CVE-2024-43117	Cross-Site Request Forgery (CSRF) vulnerability in WPMU DEV Hummingbird.This issue affects Hummingbird: from n/a through 3.9.1.	4.3	More Details
CVE-2024-43916	Authorization Bypass Through User-Controlled Key vulnerability in Dylan James Zephyr Project Manager.This issue affects Zephyr Project Manager: from n/a through 3.3.102.	4.3	More Details
CVE-2024-6688	The Oxygen Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the oxy_save_css_from_admin AJAX action in all versions up to, and including, 4.8.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update stylesheets.	4.3	More Details
CVE-2024-43340	Cross-Site Request Forgery (CSRF) vulnerability in Nasirahmed Advanced Form Integration.This issue affects Advanced Form Integration: from n/a through 1.89.4.	4.3	More Details
CVE-2024-39744	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	4.3	More Details
CVE-2024-43780	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.0, 9.8.x <= 9.8.2 fail to enforce permissions which allows a guest user with read access to upload files to a channel.	4.3	More Details
CVE-2024-43116	Cross-Site Request Forgery (CSRF) vulnerability in 10up Simple Local Avatars.This issue affects Simple Local Avatars: from n/a through 2.7.10.	4.3	More Details
CVE-2024-43356	Cross-Site Request Forgery (CSRF) vulnerability in bobbingwide.This issue affects oik: from n/a through 4.12.0.	4.3	More Details
CVE-2024-43337	Cross-Site Request Forgery (CSRF) vulnerability in Brave Brave Popup Builder.This issue affects Brave Popup Builder: from n/a through 0.7.0.	4.3	More Details
CVE-2024-6883	The Event Espresso 4 Decaf – Event Registration Event Ticketing plugin for WordPress is vulnerable to limited unauthorized plugin settings modification due to a missing capability check on the saveTimezoneString and some other functions in all versions up to, and including, 5.0.22.decaf. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify some of the plugin settings.	4.3	More Details
CVE-2024-8200	The Reviews Feed – Add Testimonials and Customer Reviews From Google Reviews, Yelp, TripAdvisor, and More plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the 'update_api_key' function. This makes it possible for unauthenticated attackers to update an API key via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8199	The Reviews Feed – Add Testimonials and Customer Reviews From Google Reviews, Yelp, TripAdvisor, and More plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_api_key' function in all versions up to, and including, 1.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update API Key options.	4.3	More Details
CVE-2024-43813	Mattermost versions 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 fail to enforce proper access controls which allows any authenticated user, including guests, to mark any channel inside any team as read for any user.	4.3	More Details
CVE-2024-5880	The Hide My Site plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2 due to the plugin not restricting access to the REST API when password protection is enabled. This makes it possible for unauthenticated attackers to gain unauthorized access to the site.	4.3	More Details
CVE-2024-43295	Cross-Site Request Forgery (CSRF) vulnerability in Passionate Programmers B.V. WP Data Access.This issue affects WP Data Access: from n/a through 5.5.7.	4.3	More Details
CVE-2024-43287	Cross-Site Request Forgery (CSRF) vulnerability in Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue.This issue affects Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue: from n/a through 3.1.82.	4.3	More Details
CVE-2024-43269	Cross-Site Request Forgery (CSRF) vulnerability in WPBackItUp Backup and Restore WordPress.This issue affects Backup and Restore WordPress: from n/a through 1.50.	4.3	More Details
CVE-2024-7030	The Smart Online Order for Clover plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.5.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update product and category descriptions, category titles and images, and sort order.	4.3	More Details
CVE-2024-7848	The User Private Files – WordPress File Sharing Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.1.0 via the 'dpk_upvf_update_doc' due to missing validation on the 'docid' user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to gain access to other user's private files.	4.3	More Details
CVE-2024-45193	An issue was discovered in Matrix libolm through 3.2.16. There is Ed25519 signature malleability due to lack of validation criteria (does not ensure that S < n). This refers to the libolm implementation of Olm. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	4.3	More Details
CVE-2024-7941	An HTTP parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.	4.3	More Details
CVE-2024-3127	An issue has been discovered in GitLab EE affecting all versions starting from 12.5 before 17.1.6, all versions starting from 17.2 before 17.2.4, all versions starting from 17.3 before 17.3.1. Under certain conditions it may be possible to bypass the IP restriction for groups through GraphQL allowing unauthorised users to perform some actions at the group level.	4.3	More Details
CVE-2024-43316	Cross-Site Request Forgery (CSRF) vulnerability in Checkout Plugins Stripe Payments For WooCommerce by Checkout.This issue affects Stripe Payments For WooCommerce by Checkout: from n/a through 1.9.1.	4.3	More Details
CVE-2024-43265	Cross-Site Request Forgery (CSRF) vulnerability in Analytify.This issue affects Analytify: from n/a through 5.3.1.	4.3	More Details
CVE-2024-43325	Cross-Site Request Forgery (CSRF) vulnerability in Naiche Dark Mode for WP Dashboard.This issue affects Dark Mode for WP Dashboard: from n/a through 1.2.3.	4.3	More Details
CVE-2024-43336	Cross-Site Request Forgery (CSRF) vulnerability in WP User Manager.This issue affects WP User Manager: from n/a through 2.9.10.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39657	Cross-Site Request Forgery (CSRF) vulnerability in Sender Sender – Newsletter, SMS and Email Marketing Automation for WooCommerce.This issue affects Sender – Newsletter, SMS and Email Marketing Automation for WooCommerce: from n/a through 2.6.18.	4.3	More Details
CVE-2024-8034	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-39641	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress LearnPress.This issue affects LearnPress: from n/a through 4.2.6.8.2.	4.3	More Details
CVE-2024-7836	The Themify Builder plugin for WordPress is vulnerable to unauthorized post duplication due to missing checks on the duplicate_page_ajaxify function in all versions up to, and including, 7.6.1. This makes it possible for authenticated attackers, with Contributor-level access and above, to duplicate and view private or draft posts created by other users that otherwise shouldn't be accessible to them.	4.3	More Details
CVE-2024-8033	Inappropriate implementation in WebApp Installs in Google Chrome on Windows prior to 128.0.6613.84 allowed an attacker who convinced a user to install a malicious application to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-7981	Inappropriate implementation in Views in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-7978	Insufficient policy enforcement in Data Transfer in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-7976	Inappropriate implementation in FedCM in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-7975	Inappropriate implementation in Permissions in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-8035	Inappropriate implementation in Extensions in Google Chrome on Windows prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-7722	Foxit PDF Reader Doc Object Use-After-Free Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-23702.	4.3	More Details
CVE-2024-42337	CyberArk - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	4.3	More Details
CVE-2024-42338	CyberArk - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	4.3	More Details
CVE-2024-42339	CyberArk - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	4.3	More Details
CVE-2024-43032	autMan v2.9.6 allows attackers to bypass authentication via a crafted web request.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43031	autMan v2.9.6 was discovered to contain an access control issue.	4.3	More Details
CVE-2024-8112	A vulnerability was found in thinkgem JeeSite 5.3. It has been rated as problematic. This issue affects some unknown processing of the file /js/a/login of the component Cookie Handler. The manipulation of the argument skinName leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-43105	Mattermost Plugin Channel Export versions <=1.0.0 fail to restrict concurrent runs of the /export command which allows a user to consume excessive resource by running the /export command multiple times at once.	4.3	More Details
CVE-2024-8165	A vulnerability, which was classified as problematic, was found in Chengdu Everbrite Network Technology BeikeShop up to 1.5.5. This affects the function exportZip of the file /admin/file_manager/export. The manipulation of the argument path leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-43319	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in bPlugins LLC Flash & HTML5 Video.This issue affects Flash & HTML5 Video: from n/a through 2.5.31.	4.3	More Details
CVE-2024-32939	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2, when shared channels are enabled, fail to redact remote users' original email addresses stored in user props when email addresses are otherwise configured not to be visible in the local server."	4.3	More Details
CVE-2024-8174	A vulnerability has been found in code-projects Blood Bank System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /login.php of the component Login Page. The manipulation of the argument user leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-41849	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could lead to a security feature bypass. An low-privileged attacker could leverage this vulnerability to slightly affect the integrity of the page. Exploitation of this issue requires user interaction and scope is changed.	4.1	More Details
CVE-2024-1544	Generating the ECDSA nonce k samples a random number r and then truncates this randomness with a modular reduction mod n where n is the order of the elliptic curve. Meaning k = r mod n. The division used during the reduction estimates a factor q_e by dividing the upper two digits (a digit having e.g. a size of 8 byte) of r by the upper digit of n and then decrements q_e in a loop until it has the correct size. Observing the number of times q_e is decremented through a control-flow revealing side-channel reveals a bias in the most significant bits of k. Depending on the curve this is either a negligible bias or a significant bias large enough to reconstruct k with lattice reduction methods. For SECP160R1, e.g., we find a bias of 15 bits.	4.1	More Details
CVE-2024-42792	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via /music/ajax.php?action=delete_playlist page.	3.5	More Details
CVE-2024-8172	A vulnerability, which was classified as problematic, has been found in SourceCodester QR Code Attendance System 1.0. This issue affects some unknown processing of the file /endpoint/delete-student.php. The manipulation of the argument student/attendance leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8022	A vulnerability was found in Genexis Tilgin Home Gateway 322_AS0500-03_05_13_05. It has been rated as problematic. This issue affects some unknown processing of the file /vood/cgi-bin/vood_view.cgi?lang=EN&act=user/spec_conf&sessionId=8621391532811654515&user=A&message2user=Account%20updated. The manipulation of the argument Phone Number leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8209	A vulnerability was found in nafisulbari/itsourcecode Insurance Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file addClient.php. The manipulation of the argument CLIENT ID leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-8208	A vulnerability has been found in nafisulbari/itsourcecode Insurance Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file editClient.php. The manipulation of the argument AGENT ID leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-8170	A vulnerability classified as problematic has been found in SourceCodester Zipped Folder Manager App 1.0. This affects an unknown part of the file /endpoint/add-folder.php. The manipulation of the argument folder leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8136	A vulnerability, which was classified as problematic, was found in SourceCodester Record Management System 1.0. This affects an unknown part of the file sort1_user.php. The manipulation of the argument position leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8140	A vulnerability was found in SourceCodester Task Progress Tracker 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file update-task.php. The manipulation of the argument task_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8141	A vulnerability was found in SourceCodester Daily Calories Monitoring Tool 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/add-calorie.php. The manipulation of the argument calorie_date/calorie_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8142	A vulnerability was found in SourceCodester Daily Calories Monitoring Tool 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /endpoint/delete-calorie.php. The manipulation of the argument calorie leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8144	A vulnerability classified as problematic was found in ClassCMS 4.8. Affected by this vulnerability is an unknown functionality of the file /index.php/admin of the component Logo Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8137	A vulnerability has been found in SourceCodester Record Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file search_user.php. The manipulation of the argument search leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8152	A vulnerability was found in SourceCodester QR Code Bookmark System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /endpoint/add-bookmark.php of the component Parameter Handler. The manipulation of the argument name/url leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8154	A vulnerability classified as problematic has been found in SourceCodester QR Code Bookmark System 1.0. Affected is an unknown function of the file /endpoint/update-bookmark.php of the component Parameter Handler. The manipulation of the argument tbl_bookmark_id/name/url leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8151	A vulnerability was found in SourceCodester Interactive Map with Marker 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/delete-mark.php. The manipulation of the argument mark leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8153	A vulnerability was found in SourceCodester QR Code Bookmark System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /endpoint/delete-bookmark.php. The manipulation of the argument bookmark leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-48937	In the Linux kernel, the following vulnerability has been resolved: io_uring: add a schedule point in io_add_buffers() Looping ~65535 times doing kmalloc() calls can trigger soft lockups, especially with DEBUG features (like KASAN). [253.536212] watchdog: BUG: soft lockup - CPU#64 stuck for 26s! [b219417889:12575] [253.544433] Modules linked in: vfat fat i2c_mux_pca954x i2c_mux spidev cdc_acm xhci_pci xhci_hcd sha3_generic gq(O) [253.544451] CPU: 64 PID: 12575 Comm: b219417889 Tainted: G S O 5.17.0-smp-DEV #801 [253.544457] RIP: 0010:kernel_text_address (./include/asm-generic/sections.h:192 ./include/linux/kallsyms.h:29 kernel/extable.c:67 kernel/extable.c:98) [253.544464] Code: 0f 93 c0 48 c7 c1 e0 63 d7 a4 48 39 cb 0f 92 c1 20 c1 0f b6 c1 5b 5d c3 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 53 48 89 fb <48> c7 c0 00 00 80 a0 41 be 01 00 00 00 48 39 c7 72 0c 48 c7 c0 40 [253.544468] RSP: 0018:ffff8882d8baf4c0 EFLAGS: 00000246 [253.544471] RAX: 1ffff1105b175e00 RBX: ffffffffa13ef09a RCX: 00000000a13ef001 [253.544474] RDX: ffffffffa13ef09a RSI: ffff8882d8baf558 RDI: ffffffffa13ef09a [253.544476] RBP: ffff8882d8baf4d8 R08: ffff8882d8baf5e0 R09: 0000000000000004 [253.544479] R10: ffff8882d8baf5e8 R11: ffffffffa0d59a50 R12: ffff8882eab20380 [253.544481] R13: ffffffffa0d59a50 R14: dfffffc0000000000 R15: 1ffff1105b175eb0 [253.544483] FS: 00000000016d3380(0000) GS:ffff88af48c00000(0000) knlGS:0000000000000000 [253.544486] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [253.544488] CR2: 00000000004af0f0 CR3: 00000002eabfa004 CR4: 00000000003706e0 [253.544491] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [253.544492] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [253.544494] Call Trace: [253.544496] <TASK> [253.544498] ? io_queue_sqe (fs/io_uring.c:7143) [253.544505] __kernel_text_address (kernel/extable.c:78) [253.544508] unwind_get_return_address (arch/x86/kernel/unwind_frame.c:19) [253.544514] arch_stack_walk (arch/x86/kernel/stacktrace.c:27) [253.544517] ? io_queue_sqe (fs/io_uring.c:7143) [253.544521] stack_trace_save (kernel/stacktrace.c:123) [253.544527] ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544531] ? ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544533] ? __kasan_kmalloc (mm/kasan/common.c:524) [253.544535] ? kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544541] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544544] ? __io_queue_sqe (fs/io_uring.c:?) [253.544551] __kasan_kmalloc (mm/kasan/common.c:524) [253.544553] kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544556] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544560] io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544564] ? __kasan_slab_alloc (mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544567] ? __kasan_slab_alloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544569] ? kmem_cache_alloc_bulk (mm/slab.h:732 mm/slab.c:3546) [253.544573] ? __io_alloc_req_refill (fs/io_uring.c:2078) [253.544578] ? io_submit_sqes (fs/io_uring.c:7441) [253.544581] ? __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uring.c:10096) [253.544584] ? __x64_sys_io_uring_enter (fs/io_uring.c:10096) [253.544587] ? do_syscall_64 (arch/x86/entry/common.c:50 arch/x86/entry/common.c:80) [253.544590] ? entry_SYSCALL_64_after_hwframe (??:?) [253.544596] __io_queue_sqe (fs/io_uring.c:?) [253.544600] io_queue_sqe (fs/io_uring.c:7143) [253.544603] io_submit_sqe (fs/io_uring.c:?) [253.544608] io_submit_sqes (fs/io_uring.c:?) [253.544612] __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uri ---truncated---	3.3	More Details
CVE-2022-48939	In the Linux kernel, the following vulnerability has been resolved: bpf: Add schedule points in batch ops syzbot reported various soft lockups caused by bpf batch operations. INFO: task kworker/1:1:27 blocked for more than 140 seconds. INFO: task hung in rcu_barrier Nothing prevents batch ops to process huge amount of data, we need to add schedule points in them. Note that maybe_wait_bpf_programs(map) calls from generic_map_delete_batch() can be factorized by moving the call after the loop. This will be done later in -next tree once we get this fix merged, unless there is strong opinion doing this optimization sooner.	3.3	More Details
CVE-2024-43411	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A theoretical vulnerability has been identified in CKEditor 4.22 (and above). In a highly unlikely scenario where an attacker gains control over the https://cke4.ckeditor.com domain, they could potentially execute an attack on CKEditor 4 instances. The issue impacts only editor instances with enabled version notifications. Please note that this feature is disabled by default in all CKEditor 4 LTS versions. Therefore, if you use CKEditor 4 LTS, it is highly unlikely that you are affected by this vulnerability. If you are unsure, please contact us. The fix is available in version 4.25.0-lts.	3.1	More Details
CVE-2024-40884	Mattermost versions 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 fail to properly enforce permissions which allows a team admin user without "Add Team Members" permission to disable the invite URL.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7998	In affected versions of Octopus Server OIDC cookies were using the wrong expiration time which could result in them using the maximum lifespan.	2.6	More Details
CVE-2024-43785	gitoxide An idiomatic, lean, fast & safe pure Rust implementation of Git. gitoxide-core, which provides most underlying functionality of the gix and ein commands, does not neutralize newlines, backspaces, or control characters—including those that form ANSI escape sequences—that appear in a repository's paths, author and committer names, commit messages, or other metadata. Such text may be written as part of the output of a command, as well as appearing in error messages when an operation fails. This sometimes allows an untrusted repository to misrepresent its contents and to alter or concoct error messages.	2.5	More Details
CVE-2024-8084	A vulnerability, which was classified as problematic, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file /php-ocls/classes/SystemSettings.php?f=update_settings of the component Setting Handler. The manipulation of the argument System Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-8145	A vulnerability, which was classified as problematic, has been found in ClassCMS 4.8. Affected by this issue is some unknown functionality of the file /index.php/admin of the component Article Handler. The manipulation of the argument Title leads to basic cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-43875	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: Clean up error handling in vpci_scan_bus() Smatch complains about inconsistent NULL checking in vpci_scan_bus(): drivers/pci/endpoint/functions/pci-epf-vntb.c:1024 vpci_scan_bus() error: we previously assumed 'vpci_bus' could be null (see line 1021) Instead of printing an error message and then crashing we should return an error code and clean up. Also the NULL check is reversed so it prints an error for success instead of failure.	N/A	More Details
CVE-2024-8088	There is a HIGH severity vulnerability affecting the CPython "zipfile" module affecting "zipfile.Path". Note that the more common API "zipfile.ZipFile" class is unaffected. When iterating over names of entries in a zip archive (for example, methods of "zipfile.Path" like "namelist()", "iterdir()", etc) the process can be put into an infinite loop with a maliciously crafted zip archive. This defect applies when reading only metadata or extracting the contents of the zip archive. Programs that are not handling user-controlled zip archives are not affected.	N/A	More Details
CVE-2024-43876	In the Linux kernel, the following vulnerability has been resolved: PCI: rcar: Demote WARN() to dev_warn_ratelimited() in rcar_pcie_wakeup() Avoid large backtrace, it is sufficient to warn the user that there has been a link problem. Either the link has failed and the system is in need of maintenance, or the link continues to work and user has been informed. The message from the warning can be looked up in the sources. This makes an actual link issue less verbose. First of all, this controller has a limitation in that the controller driver has to assist the hardware with transition to L1 link state by writing L1IATN to PMCTRL register, the L1 and L0 link state switching is not fully automatic on this controller. In case of an ASMedia ASM1062 PCIe SATA controller which does not support ASPM, on entry to suspend or during platform pm_test, the SATA controller enters D3hot state and the link enters L1 state. If the SATA controller wakes up before rcar_pcie_wakeup() was called and returns to D0, the link returns to L0 before the controller driver even started its transition to L1 link state. At this point, the SATA controller did send an PM_ENTER_L1 DLLP to the PCIe controller and the PCIe controller received it, and the PCIe controller did set PMSR PMEL1RX bit. Once rcar_pcie_wakeup() is called, if the link is already back in L0 state and PMEL1RX bit is set, the controller driver has no way to determine if it should perform the link transition to L1 state, or treat the link as if it is in L0 state. Currently the driver attempts to perform the transition to L1 link state unconditionally, which in this specific case fails with a PMSR L1FAEG poll timeout, however the link still works as it is already back in L0 state. Reduce this warning verbosity. In case the link is really broken, the rcar_pcie_config_access() would fail, otherwise it will succeed and any system with this controller and ASM1062 can suspend without generating a backtrace.	N/A	More Details
CVE-2024-43877	In the Linux kernel, the following vulnerability has been resolved: media: pci: ivtv: Add check for DMA map result In case DMA fails, 'dma->SG_length' is 0. This value is later used to access 'dma->SGarray[dma->SG_length - 1]', which will cause out of bounds access. Add check to return early on invalid value. Adjust warnings accordingly. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2024-43903	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43878	In the Linux kernel, the following vulnerability has been resolved: xfrm: Fix input error path memory access When there is a misconfiguration of input state slow path KASAN report error. Fix this error. west login: [52.987278] eth1: renamed from veth11 [53.078814] eth1: renamed from veth21 [53.181355] eth1: renamed from veth31 [54.921702] == [54.922602] BUG: KASAN: wild-memory-access in xfrmi_rcv_cb+0x2d/0x295 [54.923393] Read of size 8 at addr 6b6b6b6b00000000 by task ping/512 [54.924169] [54.924386] CPU: 0 PID: 512 Comm: ping Not tainted 6.9.0-08574-gcd29a4313a1b #25 [54.925290] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [54.926401] Call Trace: [54.926731] <IRQ> [54.927009] dump_stack_lvl+0x2a/0x3b [54.927478] kasan_report+0x84/0xa6 [54.927930] ? xfrmi_rcv_cb+0x2d/0x295 [54.928410] xfrmi_rcv_cb+0x2d/0x295 [54.928872] ? xfrm4_rcv_cb+0x3d/0x5e [54.929354] xfrm4_rcv_cb+0x46/0x5e [54.929804] xfrm_rcv_cb+0x7e/0xa1 [54.930240] xfrm_input+0x1b3a/0x1b96 [54.930715] ? xfrm_offload+0x41/0x41 [54.931182] ? raw_rcv+0x292/0x292 [54.931617] ? nf_conntrack_confirm+0xa2/0xa2 [54.932158] ? skb_sec_path+0xd/0x3f [54.932610] ? xfrmi_input+0x90/0xce [54.933066] xfrm4_esp_rcv+0x33/0x54 [54.933521] ip_protocol_deliver_rcu+0xd7/0x1b2 [54.934089] ip_local_deliver_finish+0x110/0x120 [54.934659] ? ip_protocol_deliver_rcu+0x1b2/0x1b2 [54.935248] NF_HOOK.constprop.0+0xf8/0x138 [54.935767] ? ip_sublist_rcv_finish+0x68/0x68 [54.936317] ? secure_tcpv6_ts_off+0x23/0x168 [54.936859] ? ip_protocol_deliver_rcu+0x1b2/0x1b2 [54.937454] ? __xfrm_policy_check2.constprop.0+0x18d/0x18d [54.938135] NF_HOOK.constprop.0+0xf8/0x138 [54.938663] ? ip_sublist_rcv_finish+0x68/0x68 [54.939220] ? __xfrm_policy_check2.constprop.0+0x18d/0x18d [54.939904] ? ip_local_deliver_finish+0x120/0x120 [54.940497] __netif_receive_skb_one_core+0xc9/0x107 [54.941121] ? __netif_receive_skb_list_core+0x1c2/0x1c2 [54.941771] ? blk_mq_start_stopped_hw_queues+0xc7/0xf9 [54.942413] ? blk_mq_start_stopped_hw_queue+0x38/0x38 [54.943044] ? virtqueue_get_buf_ctx+0x295/0x46b [54.943618] process_backlog+0xb3/0x187 [54.944102] __napi_poll.constprop.0+0x57/0x1a7 [54.944669] net_rx_action+0x1cb/0x380 [54.945150] ? __napi_poll.constprop.0+0x1a7/0x1a7 [54.945744] ? vring_new_virtqueue+0x17a/0x17a [54.946300] ? note_interrupt+0x2cd/0x367 [54.946805] handle_softirqs+0x13c/0x2c9 [54.947300] do_softirq+0x5f/0x7d [54.947727] </IRQ> [54.948014] <TASK> [54.948300] __local_bh_enable_ip+0x48/0x62 [54.948832] __neigh_event_send+0x3fd/0x4ca [54.949361] neigh_resolve_output+0x1e/0x210 [54.949896] ip_finish_output2+0x4bf/0x4f0 [54.950410] ? __ip_finish_output+0x171/0x1b8 [54.950956] ip_send_skb+0x25/0x57 [54.951390] raw_sendmsg+0xf95/0x10c0 [54.951850] ? check_new_pages+0x45/0x71 [54.952343] ? raw_hash_sk+0x21b/0x21b [54.952815] ? kernel_init_pages+0x42/0x51 [54.953337] ? prep_new_page+0x44/0x51 [54.953811] ? get_page_from_freelist+0x72b/0x915 [54.954390] ? signal_pending_state+0x77/0x77 [54.954936] ? preempt_count_sub+0x14/0xb3 [54.955450] ? __might_resched+0x8a/0x240 [54.955951] ? __might_sleep+0x25/0xa0 [54.956424] ? first_zones_zonelist+0x2c/0x43 [54.956977] ? __rcu_read_lock+0x2d/0x3a [54.957476] ? __pte_offset_map+0x32/0xa4 [54.957980] ? __might_resched+0x8a/0x240 [54.958483] ? __might_sleep+0x25/0xa0 [54.958963] ? inet_send_prepare+0x54/0x54 [54.959478] ? sock_sendmsg_nosec+0x42/0x6c [54.960000] sock_sendmsg_nosec+0x42/0x6c [54.960502] __sys_sendto+0x15d/0x1cc [54.960966] ? __x64_sys_getpeername+0x44/0x44 [54.961522] ? __handle_mm_fault+0x679/0xae4 [54.962068] ? find_vma+0x6b/0x ---truncated---	N/A	More Details
CVE-2024-43898	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-7987	A remote code execution vulnerability exists in the Rockwell Automation ThinManager® ThinServer™ that allows a threat actor to execute arbitrary code with System privileges. To exploit this vulnerability and a threat actor must abuse the ThinServer™ service by creating a junction and use it to upload arbitrary files.	N/A	More Details
CVE-2024-43870	In the Linux kernel, the following vulnerability has been resolved: perf: Fix event leak upon exit When a task is scheduled out, pending sigtrap deliveries are deferred to the target task upon resume to userspace via task_work. However failures while adding an event's callback to the task_work engine are ignored. And since the last call for events exit happen after task work is eventually closed, there is a small window during which pending sigtrap can be queued though ignored, leaking the event refcount addition such as in the following scenario: TASK A ----- do_exit() exit_task_work(tsk); <IRQ> perf_event_overflow() event->pending_sigtrap = pending_id; irq_work_queue(&event->pending_irq); </IRQ> ==========> PREEMPTION: TASK A -> TASK B event_sched_out() event->pending_sigtrap = 0; atomic_long_inc_not_zero(&event->refcount) // FAILS: task work has exited task_work_add(&event->pending_task) [...] <IRQ WORK> perf_pending_irq() // early return: event->oncpu = -1 </IRQ WORK> [...] ==========> TASK B -> TASK A perf_event_exit_task(tsk) perf_event_exit_event() free_event() WARN(atomic_long_cmpxchg(&event->refcount, 1, 0) != 1) // leak event due to unexpected refcount == 2 As a result the event is never released while the task exits. Fix this with appropriate task_work_add()'s error handling.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43869	In the Linux kernel, the following vulnerability has been resolved: perf: Fix event leak upon exec and file release The perf pending task work is never waited upon the matching event release. In the case of a child event, released via free_event() directly, this can potentially result in a leaked event, such as in the following scenario that doesn't even require a weak IRQ work implementation to trigger: schedule() prepare_task_switch() =======> <NMI> perf_event_overflow() event->pending_sigtrap = ... irq_work_queue(&event->pending_irq) <======= </NMI> perf_event_task_sched_out() event_sched_out() event->pending_sigtrap = 0; atomic_long_inc_not_zero(&event->refcount) task_work_add(&event->pending_task) finish_lock_switch() =======> <IRQ> perf_pending_irq() //do nothing, rely on pending task work <======= </IRQ> begin_new_exec() perf_event_exit_task() perf_event_exit_event() // If is child event free_event() WARN(atomic_long_cmpxchg(&event->refcount, 1, 0) != 1) // event is leaked Similar scenarios can also happen with perf_event_remove_on_exec() or simply against concurrent perf_event_release(). Fix this with synchonizing against the possibly remaining pending task work while freeing the event, just like is done with remaining pending IRQ work. This means that the pending task callback neither need nor should hold a reference to the event, preventing it from ever beeing freed.	N/A	More Details
CVE-2024-43885	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-7986	A vulnerability exists in the Rockwell Automation ThinManager® ThinServer that allows a threat actor to disclose sensitive information. A threat actor can exploit this vulnerability by abusing the ThinServer™ service to read arbitrary files by creating a junction that points to the target directory.	N/A	More Details
CVE-2024-43868	In the Linux kernel, the following vulnerability has been resolved: riscv/purgatory: align riscv_kernel_entry When alignment handling is delegated to the kernel, everything must be word-aligned in purgatory, since the trap handler is then set to the kexec one. Without the alignment, hitting the exception would ultimately crash. On other occasions, the kernel's handler would take care of exceptions. This has been tested on a JH7110 SoC with oreboot and its SBI delegating unaligned access exceptions and the kernel configured to handle them.	N/A	More Details
CVE-2024-43867	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: prime: fix refcount underflow Calling nouveau_bo_ref() on a nouveau_bo without initializing it (and hence the backing ttm_bo) leads to a refcount underflow. Instead of calling nouveau_bo_ref() in the unwind path of drm_gem_object_init(), clean things up manually. (cherry picked from commit 1b93f3e89d03cfc576636e195466a0d728ad8de5)	N/A	More Details
CVE-2024-43866	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Always drain health in shutdown callback There is no point in recovery during device shutdown. if health work started need to wait for it to avoid races and NULL pointer access. Hence, drain health WQ on shutdown callback.	N/A	More Details
CVE-2024-43865	In the Linux kernel, the following vulnerability has been resolved: s390/fpu: Re-add exception handling in load_fpu_state() With the recent rewrite of the fpu code exception handling for the lfpc instruction within load_fpu_state() was erroneously removed. Add it again to prevent that loading invalid floating point register values cause an unhandled specification exception.	N/A	More Details
CVE-2024-43864	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix CT entry update leaks of modify header context The cited commit allocates a new modify header to replace the old one when updating CT entry. But if failed to allocate a new one, eg. exceed the max number firmware can support, modify header will be an error pointer that will trigger a panic when deallocating it. And the old modify header point is copied to old attr. When the old attr is freed, the old modify header is lost. Fix it by restoring the old attr to attr when failed to allocate a new modify header context. So when the CT entry is freed, the right modify header context will be freed. And the panic of accessing error pointer is also fixed.	N/A	More Details
CVE-2024-5814	A malicious TLS1.2 server can force a TLS1.3 client with downgrade capability to use a ciphersuite that it did not agree to and achieve a successful connection. This is because, aside from the extensions, the client was skipping fully parsing the server hello. https://doi.org/10.46586/tches.v2024.i1.457-500	N/A	More Details
CVE-2024-7989	Rejected reason: Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that the issue does not pose a security risk as it falls within the expected functionality and security controls of the application. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-43879	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: handle 2x996 RU allocation in cfg80211_calculate_bitrate_he() Currently NL80211_RATE_INFO_HE_RU_ALLOC_2x996 is not handled in cfg80211_calculate_bitrate_he(), leading to below warning: kernel: invalid HE MCS: bw:6, ru:6 kernel: WARNING: CPU: 0 PID: 2312 at net/wireless/util.c:1501 cfg80211_calculate_bitrate_he+0x22b/0x270 [cfg80211] Fix it by handling 2x996 RU allocation in the same way as 160 MHz bandwidth.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43883	In the Linux kernel, the following vulnerability has been resolved: usb: vhci-hcd: Do not drop references before new references are gained At a few places the driver carries stale pointers to references that can still be used. Make sure that does not happen. This strictly speaking closes ZDI-CAN-22273, though there may be similar races in the driver.	N/A	More Details
CVE-2024-42992	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-48936	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-8188	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-48880	In the Linux kernel, the following vulnerability has been resolved: platform/surface: aggregator: Add missing call to ssam_request_sync_free() Although rare, ssam_request_sync_init() can fail. In that case, the request should be freed via ssam_request_sync_free(). Currently it is leaked instead. Fix this.	N/A	More Details
CVE-2024-7427	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText™ Network Node Manager i (NNMi) could allow Cross-Site Scripting (XSS).This issue affects Network Node Manager i (NNMi): 2022.11, 2023.05, 23.4, 24.2.	N/A	More Details
CVE-2022-48883	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: IPoIB, Block PKEY interfaces with less rx queues than parent A user is able to configure an arbitrary number of rx queues when creating an interface via netlink. This doesn't work for child PKEY interfaces because the child interface uses the parent receive channels. Although the child shares the parent's receive channels, the number of rx queues is important for the channel_stats array: the parent's rx channel index is used to access the child's channel_stats. So the array has to be at least as large as the parent's rx queue size for the counting to work correctly and to prevent out of bound accesses. This patch checks for the mentioned scenario and returns an error when trying to create the interface. The error is propagated to the user.	N/A	More Details
CVE-2022-48900	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-7757	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43880	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_acl_erp: Fix object nesting warning ACLs in Spectrum-2 and newer ASICs can reside in the algorithmic TCAM (A-TCAM) or in the ordinary circuit TCAM (C-TCAM). The former can contain more ACLs (i.e., tc filters), but the number of masks in each region (i.e., tc chain) is limited. In order to mitigate the effects of the above limitation, the device allows filters to share a single mask if their masks only differ in up to 8 consecutive bits. For example, dst_ip/25 can be represented using dst_ip/24 with a delta of 1 bit. The C-TCAM does not have a limit on the number of masks being used (and therefore does not support mask aggregation), but can contain a limited number of filters. The driver uses the "objagg" library to perform the mask aggregation by passing it objects that consist of the filter's mask and whether the filter is to be inserted into the A-TCAM or the C-TCAM since filters in different TCAMs cannot share a mask. The set of created objects is dependent on the insertion order of the filters and is not necessarily optimal. Therefore, the driver will periodically ask the library to compute a more optimal set ("hints") by looking at all the existing objects. When the library asks the driver whether two objects can be aggregated the driver only compares the provided masks and ignores the A-TCAM / C-TCAM indication. This is the right thing to do since the goal is to move as many filters as possible to the A-TCAM. The driver also forbids two identical masks from being aggregated since this can only happen if one was intentionally put in the C-TCAM to avoid a conflict in the A-TCAM. The above can result in the following set of hints: H1: {mask X, A-TCAM} -> H2: {mask Y, A-TCAM} // X is Y + delta H3: {mask Y, C-TCAM} -> H4: {mask Z, A-TCAM} // Y is Z + delta After getting the hints from the library the driver will start migrating filters from one region to another while consulting the computed hints and instructing the device to perform a lookup in both regions during the transition. Assuming a filter with mask X is being migrated into the A-TCAM in the new region, the hints lookup will return H1. Since H2 is the parent of H1, the library will try to find the object associated with it and create it if necessary in which case another hints lookup (recursive) will be performed. This hints lookup for {mask Y, A-TCAM} will either return H2 or H3 since the driver passes the library an object comparison function that ignores the A-TCAM / C-TCAM indication. This can eventually lead to nested objects which are not supported by the library [1]. Fix by removing the object comparison function from both the driver and the library as the driver was the only user. That way the lookup will only return exact matches. I do not have a reliable reproducer that can reproduce the issue in a timely manner, but before the fix the issue would reproduce in several minutes and with the fix it does not reproduce in over an hour. Note that the current usefulness of the hints is limited because they include the C-TCAM indication and represent aggregation that cannot actually happen. This will be addressed in net-next. [1] WARNING: CPU: 0 PID: 153 at lib/objagg.c:170 objagg_obj_parent_assign+0xb5/0xd0 Modules linked in: CPU: 0 PID: 153 Comm: kworker/0:18 Not tainted 6.9.0-rc6-custom-g70fbc2c1c38b #42 Hardware name: Mellanox Technologies Ltd. MSN3700C/VMOD0008, BIOS 5.11 10/10/2018 Workqueue: mlxsw_core mlxsw_sp_acl_tcam_vregion_rehash_work RIP: 0010:objagg_obj_parent_assign+0xb5/0xd0 [...] Call Trace: <TASK> __objagg_obj_get+0x2bb/0x580 objagg_obj_get+0xe/0x80 mlxsw_sp_acl_erp_mask_get+0xb5/0xf0 mlxsw_sp_acl_atcam_entry_add+0xe8/0x3c0 mlxsw_sp_acl_tcam_entry_create+0x5e/0xa0 mlxsw_sp_acl_tcam_vchunk_migrate_one+0x16b/0x270 mlxsw_sp_acl_tcam_vregion_rehash_work+0xbe/0x510 process_one_work+0x151/0x370	N/A	More Details
CVE-2022-26327	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in OpenText Performance Center on Windows allows Retrieve Embedded Sensitive Data.This issue affects Performance Center: 12.63.	N/A	More Details
CVE-2022-26328	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText Performance Center on Windows allows Cross-Site Scripting (XSS).This issue affects Performance Center: 12.63.	N/A	More Details
CVE-2024-45036	Tophat is a mobile applications testing harness. An Improper Access Control vulnerability can expose the `TOPHAT_APP_TOKEN` token stored in `~/.tophatrc` through use of a malicious Tophat URL controlled by the attacker. The vulnerability allows Tophat to send this token to the attacker's server without any checks to ensure that the server is trusted. This token can then be used to access internal build artifacts, for mobile applications, not intended to be public. The issue has been patched as of version 1.10.0. The ability to request artifacts using a Tophat API has been deprecated as this flow was inherently insecure. Systems that have implemented this kind of endpoint should cease use and invalidate the token immediately. There are no workarounds and all users should update as soon as possible.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21690	This High severity Reflected XSS and CSRF (Cross-Site Request Forgery) vulnerability was introduced in versions 7.19.0, 7.20.0, 8.0.0, 8.1.0, 8.2.0, 8.3.0, 8.4.0, 8.5.0, 8.6.0, 8.7.1, 8.8.0, and 8.9.0 of Confluence Data Center and Server. This Reflected XSS and CSRF (Cross-Site Request Forgery) vulnerability, with a CVSS Score of 7.1, allows an unauthenticated attacker to execute arbitrary HTML or JavaScript code on a victims browser and force a end user to execute unwanted actions on a web application in which they're currently authenticated which has high impact to confidentiality, low 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: * Confluence Data Center and Server 7.19: Upgrade to a release greater than or equal to 7.19.26 * Confluence Data Center and Server 8.5: Upgrade to a release greater than or equal to 8.5.14 * Confluence Data Center and Server 9.0: Upgrade to a release greater than or equal to 9.0.1 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-2022-48884	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix command stats access after free Command may fail while driver is reloading and can't accept FW commands till command interface is reinitialized. Such command failure is being logged to command stats. This results in NULL pointer access as command stats structure is being freed and reallocated during mlx5 devlink reload (see kernel log below). Fix it by making command stats statically allocated on driver probe. Kernel log: [2394.808802] BUG: unable to handle kernel paging request at 000000000002a9c0 [2394.810610] PGD 0 P4D 0 [2394.811811] Oops: 0002 [#1] SMP NOPTI ... [2394.815482] RIP: 0010:native_queued_spin_lock_slowpath+0x183/0x1d0 ... [2394.829505] Call Trace: [2394.830667] _raw_spin_lock_irq+0x23/0x26 [2394.831858] cmd_status_err+0x55/0x110 [mlx5_core] [2394.833020] mlx5_access_reg+0xe7/0x150 [mlx5_core] [2394.834175] mlx5_query_port_ptys+0x78/0xa0 [mlx5_core] [2394.835337] mlx5e_ethtool_get_link_ksettings+0x74/0x590 [mlx5_core] [2394.836454] ? kmem_cache_alloc_trace+0x140/0x1c0 [2394.837562] __rh_call_get_link_ksettings+0x33/0x100 [2394.838663] ? __rtnl_unlock+0x25/0x50 [2394.839755] __ethtool_get_link_ksettings+0x72/0x150 [2394.840862] duplex_show+0x6e/0xc0 [2394.841963] dev_attr_show+0x1c/0x40 [2394.843048] sysfs_kf_seq_show+0x9b/0x100 [2394.844123] seq_read+0x153/0x410 [2394.845187] vfs_read+0x91/0x140 [2394.846226] ksys_read+0x4f/0xb0 [2394.847234] do_syscall_64+0x5b/0x1a0 [2394.848228] entry_SYSCALL_64_after_hwframe+0x65/0xca	N/A	More Details
CVE-2024-43881	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: change DMA direction while mapping reinjected packets For fragmented packets, ath12k reassembles each fragment as a normal packet and then reinjects it into HW ring. In this case, the DMA direction should be DMA_TO_DEVICE, not DMA_FROM_DEVICE. Otherwise, an invalid payload may be reinjected into the HW and subsequently delivered to the host. Given that arbitrary memory can be allocated to the skb buffer, knowledge about the data contained in the reinjected buffer is lacking. Consequently, there’s a risk of private information being leaked. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.1.1-00209-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2024-7428	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in OpenText™ Network Node Manager i (NNMi) allows URL Redirector Abuse.This issue affects Network Node Manager i (NNMi): 2022.11, 2023.05, 23.4, 24.2.	N/A	More Details
CVE-2024-8197	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-7859. Reason: This candidate is a reservation duplicate of CVE-2024-7859. Notes: All CVE users should reference CVE-2024-7859 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details