SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 May 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-2024-5407	A vulnerability in RhinOS 3.0-1190 could allow PHP code injection through the "search" parameter in /portal/search.htm. This vulnerability could allow a remote attacker to perform a reverse shell on the remote system, compromising the entire infrastructure.	10.0	More Details
CVE-2024-33226	An issue in the component Access64.sys of Wistron Corporation TBT Force Power Control v1.0.0.0 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	9.9	More Details
CVE-2024-35344	Certain Anpviz products contain a hardcoded cryptographic key stored in the firmware of the device. This affects IPC-D250, IPC-D260, IPC-B850, IPC-D850, IPC-D350, IPC-D3150, IPC-D4250, IPC-D380, IPC-D880, IPC-D280, IPC-D3180, MC800N, YM500L, YM800N_N2, YMF50B, YM800SV2, YM500L8, and YM200E10 firmware v3.2.2.2 and lower and possibly more vendors/models of IP camera.	9.9	More Details
CVE-2024-4443	The Business Directory Plugin – Easy Listing Directories for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'listingfields' parameter in all versions up to, and including, 6.4.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2024-24963	A stack-based buffer overflow vulnerability exists in the Programming Software Connection FileSelect functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to stack-based buffer overflow. An attacker can send an unauthenticated packet to trigger this vulnerability.This CVE tracks the stack-based buffer overflow that occurs at offset `0xb6e84` of v1.2.10.9 of the P3-550E firmware.	9.8	More Details
CVE-2024-35396	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a hardcoded password for telnet in /web_cste/cgi-bin/product.ini, which allows attackers to log in as root.	9.8	More Details
CVE-2024-35387	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the http_host parameter in the function loginAuth.	9.8	More Details
CVE-2024-35373	Mocodo Mocodo Online 4.2.6 and below is vulnerable to Remote Code Execution via /web/rewrite.php.	9.8	More Details
CVE-2024-35374	Mocodo Mocodo Online 4.2.6 and below does not properly sanitize the sql_case input field in /web/generate.php, allowing remote attackers to execute arbitrary commands and potentially command injection, leading to remote code execution (RCE) under certain conditions.	9.8	More Details
CVE-2024-26289	Deserialization of Untrusted Data vulnerability in PMB Services PMB allows Remote Code Inclusion.This issue affects PMB: from 7.5.1 before 7.5.6-2, from 7.4.1 before 7.4.9, from 7.3.1 before 7.3.18.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35398	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a stack overflow via the desc parameter in the function setMacFilterRules.	9.8	More Details
CVE-2024-21785	A leftover debug code vulnerability exists in the Telnet Diagnostic Interface functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted series of network requests can lead to unauthorized access. An attacker can send a sequence of requests to trigger this vulnerability.	9.8	More Details
CVE-2024-23601	A code injection vulnerability exists in the scan_lib.bin functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted scan_lib.bin can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2024-24962	A stack-based buffer overflow vulnerability exists in the Programming Software Connection FileSelect functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to stack-based buffer overflow. An attacker can send an unauthenticated packet to trigger this vulnerability.This CVE tracks the stack-based buffer overflow that occurs at offset `0xb6e98` of v1.2.10.9 of the P3-550E firmware.	9.8	More Details
CVE-2024-33800	A SQL injection vulnerability in /model/get_student1.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the index parameter.	9.8	More Details
CVE-2024-33799	A SQL injection vulnerability in /model/get_teacher.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-31510	An issue in Open Quantum Safe liboqs v.10.0 allows a remote attacker to escalate privileges via the crypto_sign_signature parameter in the /pqcrystals-dilithium-standard_ml-dsa-44-ipd_avx2/sign.c component.	9.8	More Details
CVE-2024-33801	A SQL injection vulnerability in /model/get_subject_routing.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-33805	A SQL injection vulnerability in /model/get_student.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-33806	A SQL injection vulnerability in /model/get_grade.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-33808	A SQL injection vulnerability in /model/get_timetable.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-35324	Douchat 4.0.5 suffers from an arbitrary file upload vulnerability via Public/Plugins/webuploader/server/preview.php.	9.8	More Details
CVE-2024-34854	F-logic DataCube3 v1.0 is vulnerable to File Upload via `/admin/transceiver_schedule.php.`	9.8	More Details
CVE-2024-35343	Certain Anpviz products allow unauthenticated users to download arbitrary files from the device's filesystem via a HTTP GET request to the /playback/ URI. This affects IPC-D250, IPC-D260, IPC-B850, IPC-D850, IPC-D350, IPC-D3150, IPC-D4250, IPC-D380, IPC-D880, IPC-D280, IPC-D3180, MC800N, YM500L, YM800N_N2, YMF50B, YM800SV2, YM500L8, and YM200E10 (IP Cameras) firmware v3.2.2.2 and lower and possibly more vendors/models of IP camera.	9.8	More Details
CVE-2024-35563	CDG-Server-V5.6.2.126.139 and earlier was discovered to contain a SQL injection vulnerability via the permissionId parameter in CDGTempPermissions.	9.8	More Details
CVE-2023-43845	Aten PE6208 2.3.228 and 2.4.232 have default credentials for the privileged telnet account. The user is not asked to change the credentials after first login. If not changed, attackers can log in to the telnet console and gain administrator privileges.	9.8	More Details
CVE-2024-5147	The WPZOOM Addons for Elementor (Templates, Widgets) plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.37 via the 'grid_style' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	9.8	More Details
CVE-2024-35339	Tenda FH1206 V1.2.0.8(8155) was discovered to contain a command injection vulnerability via the mac parameter at ip/goform/WriteFacMac.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47548	In the Linux kernel, the following vulnerability has been resolved: ethernet: hisilicon: hns: hns_dsaf_misc: fix a possible array overflow in hns_dsaf_ge_srst_by_port() The if statement: if (port >= DSAF_GE_NUM) return; limits the value of port less than DSAF_GE_NUM (i.e., 8). However, if the value of port is 6 or 7, an array overflow could occur: port_rst_off = dsaf_dev->mac_cb[port]->port_rst_off; because the length of dsaf_dev->mac_cb is DSAF_MAX_PORT_NUM (i.e., 6). To fix this possible array overflow, we first check port and if it is greater than or equal to DSAF_MAX_PORT_NUM, the function returns.	9.8	More Details
CVE-2024-35086	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in BpmTaskFromMapper.xml .	9.8	More Details
CVE-2024-3495	The Country State City Dropdown CF7 plugin for WordPress is vulnerable to SQL Injection via the ‘cnt’ and 'sid' parameters in versions up to, and including, 2.7.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2024-35409	WeBid 1.1.2 is vulnerable to SQL Injection via admin/tax.php.	9.8	More Details
CVE-2024-5168	Improper access control vulnerability in Prodys' Quantum Audio codec affecting versions 2.3.4t and below. This vulnerability could allow an unauthenticated user to bypass authentication entirely and execute arbitrary API requests against the web application.	9.8	More Details
CVE-2024-5084	The Hash Form – Drag & Drop Form Builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'file_upload_action' function in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-34927	A SQL injection vulnerability in /model/update_classroom.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the name parameter.	9.8	More Details
CVE-2024-34929	A SQL injection vulnerability in /view/find_friends.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the my_index parameter.	9.8	More Details
CVE-2024-34931	A SQL injection vulnerability in /model/update_subject.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the name parameter.	9.8	More Details
CVE-2024-34932	A SQL injection vulnerability in /model/update_exam.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the name parameter.	9.8	More Details
CVE-2024-34934	A SQL injection vulnerability in /view/emarks_range_grade_update_form.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the conversation_id parameter.	9.8	More Details
CVE-2024-34935	A SQL injection vulnerability in /view/conversation_history_admin.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the conversation_id parameter.	9.8	More Details
CVE-2024-35084	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in SysMsgPushMapper.xml.	9.8	More Details
CVE-2024-35091	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in SysTenantMapper.xml.	9.8	More Details
CVE-2024-35079	An arbitrary file upload vulnerability in the uploadAudio method of inxedu v2024.4 allows attackers to execute arbitrary code via uploading a crafted .jsp file.	9.8	More Details
CVE-2024-35080	An arbitrary file upload vulnerability in the gok4 method of inxedu v2024.4 allows attackers to execute arbitrary code via uploading a crafted .jsp file.	9.8	More Details
CVE-2024-35375	There is an arbitrary file upload vulnerability on the media add .php page in the backend of the website in version 5.7.114 of DedeCMS	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35570	An arbitrary file upload vulnerability in the component \controller\ImageUploadController.class of inxedu v2.0.6 allows attackers to execute arbitrary code via uploading a crafted jsp file.	9.8	More Details
CVE-2024-4544	The Pie Register - Social Sites Login (Add on) plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.7.7. This is due to insufficient verification on the user being supplied during a social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	9.8	More Details
CVE-2024-35510	An arbitrary file upload vulnerability in /dede/file_manage_control.php of DedeCMS v5.7.114 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2024-35592	An arbitrary file upload vulnerability in the Upload function of Box-IM v2.0 allows attackers to execute arbitrary code via uploading a crafted PDF file.	9.6	More Details
CVE-2024-5274	Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2024-22590	The TLS engine in Kwik commit 745fd4e2 does not track the current state of the connection. This vulnerability can allow Client Hello messages to be overwritten at any time, including after a connection has been established.	9.1	More Details
CVE-2024-22187	A write-what-where vulnerability exists in the Programming Software Connection Remote Memory Diagnostics functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to an arbitrary write. An attacker can send an unauthenticated packet to trigger this vulnerability.	9.1	More Details
CVE-2024-4399	The does not validate a parameter before making a request to it, which could allow unauthenticated users to perform SSRF attack	9.1	More Details
CVE-2024-25738	A Server-Side Request Forgery (SSRF) vulnerability in the /Upgrade/FixConfig route in Open Library Foundation VuFind 2.0 through 9.1 before 9.1.1 allows a remote attacker to overwrite local configuration files to gain access to the administrator panel and achieve Remote Code Execution. A mitigating factor is that it requires the allow_url_include PHP runtime setting to be on, which is off in default installations. It also requires the /Upgrade route to be exposed, which is exposed by default after installing VuFind, and is recommended to be disabled by setting autoConfigure to false in config.ini.	9.1	More Details
CVE-2024-5314	Vulnerabilities in Dolibarr ERP - CRM that affect version 9.0.1 and allow SQL injection. These vulnerabilities could allow a remote attacker to send a specially crafted SQL query to the system and retrieve all the information stored in the database through the parameters sortorder y sortfield in /dolibarr/admin/dict.php.	9.1	More Details
CVE-2024-5315	Vulnerabilities in Dolibarr ERP - CRM that affect version 9.0.1 and allow SQL injection. These vulnerabilities could allow a remote attacker to send a specially crafted SQL query to the system and retrieve all the information stored in the database through the parameters viewstatut in /dolibarr/commande/list.php.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-3518	The Media Library Assistant plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode(s) in all versions up to, and including, 3.15 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor access or higher, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-23950	Multiple improper array index validation vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the `igl::MshLoader::parse_element_field` function while handling an `binary`.msh` file.	8.8	More Details
CVE-2024-23947	Multiple improper array index validation vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the `igl::MshLoader::parse_nodes` function while handling a `binary` `.msh` file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45171	An issue was discovered in LIVEBOX Collaboration vDesk through v018. An Unrestricted Upload of a File with a Dangerous Type can occur under the vShare web site section. A remote user, authenticated to the product, can arbitrarily upload potentially dangerous files without restrictions.	8.8	More Details
CVE-2024-34448	Ghost before 5.82.0 allows CSV Injection during a member CSV export.	8.8	More Details
CVE-2024-33227	An issue in the component ddcdrv.sys of Nicomsoft WinI2C/DDC v3.7.4.0 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	8.8	More Details
CVE-2024-23951	Multiple improper array index validation vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the `igl::MshLoader::parse_element_field` function while handling an `ascii`.msh` file.	8.8	More Details
CVE-2024-33223	An issue in the component IOMap64.sys of ASUSTeK Computer Inc ASUS GPU TweakII v1.4.5.2 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	8.8	More Details
CVE-2024-33220	An issue in the component AsIO3_64.sys of ASUSTeK Computer Inc AISuite3 v3.03.36 3.03.36 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	8.8	More Details
CVE-2024-5160	Heap buffer overflow in Dawn in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-35559	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoMove_deal.php?mudi=rev&nohrefStr=close.	8.8	More Details
CVE-2024-35558	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/ca_deal.php?mudi=rev&nohrefStr=close.	8.8	More Details
CVE-2024-35556	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/vpsSys_deal.php?mudi=infoSet.	8.8	More Details
CVE-2024-23949	Multiple improper array index validation vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the `igl::MshLoader::parse_node_field` function while handling an `ascii`.msh` file.	8.8	More Details
CVE-2024-35552	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoMove_deal.php?mudi=del&dataType=logo&dataTypeCN.	8.8	More Details
CVE-2024-5400	Openfind Mail2000 does not properly filter parameters of specific CGI. Remote attackers with regular privileges can exploit this vulnerability to execute arbitrary system commands on the remote server.	8.8	More Details
CVE-2024-5159	Heap buffer overflow in ANGLE in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5157	Use after free in Scheduling in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36077	Qlik Sense Enterprise for Windows before 14.187.4 allows a remote attacker to elevate their privilege due to improper validation. The attacker can elevate their privilege to the internal system role, which allows them to execute commands on the server. This affects February 2024 Patch 3 (14.173.3 through 14.173.7), November 2023 Patch 8 (14.159.4 through 14.159.13), August 2023 Patch 13 (14.139.3 through 14.139.20), May 2023 Patch 15 (14.129.3 through 14.129.22), February 2023 Patch 13 (14.113.1 through 14.113.18), November 2022 Patch 13 (14.97.2 through 14.97.18), August 2022 Patch 16 (14.78.3 through 14.78.23), and May 2022 Patch 17 (14.67.7 through 14.67.31). This has been fixed in May 2024 (14.187.4), February 2024 Patch 4 (14.173.8), November 2023 Patch 9 (14.159.14), August 2023 Patch 14 (14.139.21), May 2023 Patch 16 (14.129.23), February 2023 Patch 14 (14.113.19), November 2022 Patch 14 (14.97.19), August 2022 Patch 17 (14.78.25), and May 2022 Patch 18 (14.67.34).	8.8	More Details
CVE-2024-35186	gitoxide is a pure Rust implementation of Git. During checkout, `gix-worktree-state` does not verify that paths point to locations in the working tree. A specially crafted repository can, when cloned, place new files anywhere writable by the application. This vulnerability leads to a major loss of confidentiality, integrity, and availability, but creating files outside a working tree without attempting to execute code can directly impact integrity as well. This vulnerability has been patched in version(s) 0.36.0.	8.8	More Details
CVE-2024-35083	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in SysLoginInfoMapper.xml.	8.8	More Details
CVE-2024-5201	Privilege Escalation in OpenText Dimensions RM allows an authenticated user to escalate there privilege to the privilege of another user via HTTP Request	8.8	More Details
CVE-2024-5246	NETGEAR ProSAFE Network Management System Tomcat 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 product installer. The issue results from the use of a vulnerable version of Apache Tomcat. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22868.	8.8	More Details
CVE-2024-34060	IrisEVTXModule is an interface module for Evtx2Splunk and Iris in order to ingest Microsoft EVTX log files. The `iris-evtx-module` is a pipeline plugin of `iris-web` that processes EVTX files through IRIS web application. During the upload of an EVTX through this pipeline, the filename is not safely handled and may cause an Arbitrary File Write. This can lead to a remote code execution (RCE) when combined with a Server Side Template Injection (SSTI). This vulnerability has been patched in version 1.0.0.	8.8	More Details
CVE-2024-35399	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a stack overflow via the password parameter in the function loginAuth	8.8	More Details
CVE-2024-20360	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface does not adequately validate user input. An attacker could exploit this vulnerability by authenticating to the application and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to obtain any data from the database, execute arbitrary commands on the underlying operating system, and elevate privileges to root. To exploit this vulnerability, an attacker would need at least Read Only user credentials.	8.8	More Details
CVE-2024-4779	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to SQL Injection via the 'data[post_ids][0]' parameter in all versions up to, and including, 1.5.107 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-35395	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a hardcoded password vulnerability in /etc/shadow.sample, which allows attackers to log in as root.	8.8	More Details
CVE-2024-4662	The Oxygen Builder plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.8.2 via post metadata. This is due to the plugin storing custom data in post metadata without an underscore prefix. This makes it possible for lower privileged users, such as contributors, to inject arbitrary PHP code via the WordPress user interface and gain elevated privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35388	TOTOLINK NR1800X v9.1.0u.6681_B20230703 was discovered to contain a stack overflow via the password parameter in the function urldecode	8.8	More Details
CVE-2024-35397	TOTOLINK CP900L v4.1.5cu.798_B20221228 weas discovered to contain a command injection vulnerability in the NTPSyncWithHost function via the hostTime parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	8.8	More Details
CVE-2024-23948	Multiple improper array index validation vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the `igl::MshLoader::parse_nodes` function while handling an `ascii`.msh` file.	8.8	More Details
CVE-2024-35340	Tenda FH1206 V1.2.0.8(8155) was discovered to contain a command injection vulnerability via the cmdinput parameter at ip/goform/formexeCommand.	8.6	More Details
CVE-2024-24919	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available.	8.6	More Details
CVE-2024-34936	A SQL injection vulnerability in /view/event1.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the month parameter.	8.6	More Details
CVE-2024-35231	rack-contrib provides contributed rack middleware and utilities for Rack, a Ruby web server interface. Versions of rack-contrib prior to 2.5.0 are vulnerable to denial of service due to the fact that the user controlled data `profiler_runs` was not constrained to any limitation. This would lead to allocating resources on the server side with no limitation and a potential denial of service by remotely user-controlled data. Version 2.5.0 contains a patch for the issue.	8.6	More Details
CVE-2024-2088	The NextScripts: Social Networks Auto-Poster plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.4.3 via the 'nxs_getExpSettings' function. This makes it possible for authenticated attackers, with subscriber access and above, to extract sensitive data including social network API keys and secrets.	8.5	More Details
CVE-2024-5031	The Memberpress plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 1.11.29 via the 'mepr-user-file' shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	8.5	More Details
CVE-2021-47456	In the Linux kernel, the following vulnerability has been resolved: can: peak_pci: peak_pci_remove(): fix UAF When remove the module peek_pci, referencing 'chan' again after releasing 'dev' will cause UAF. Fix this by releasing 'dev' later. The following log reveals it: [35.961814] BUG: KASAN: use-after-free in peak_pci_remove+0x16f/0x270 [peak_pci] [35.963414] Read of size 8 at addr ffff888136998ee8 by task modprobe/5537 [35.965513] Call Trace: [35.965718] dump_stack_lvl+0xa8/0xd1 [35.966028] print_address_description+0x87/0x3b0 [35.966420] kasan_report+0x172/0x1c0 [35.966725] ? peak_pci_remove+0x16f/0x270 [peak_pci] [35.967137] ? trace_irq_enable_rcuidle+0x10/0x170 [35.967529] ? peak_pci_remove+0x16f/0x270 [peak_pci] [35.967945] __asan_report_load8_noabort+0x14/0x20 [35.968346] peak_pci_remove+0x16f/0x270 [peak_pci] [35.968752] pci_device_remove+0xa9/0x250	8.4	More Details
CVE-2024-33224	An issue in the component rtkio64.sys of Realtek Semiconductor Corp Realtek IO Driver v1.008.0823.2017 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	8.4	More Details
CVE-2024-28886	OS command injection vulnerability exists in UTAU versions prior to v0.4.19. If a user of the product opens a crafted UTAU project file (.ust file), an arbitrary OS command may be executed.	8.4	More Details
CVE-2024-26024	SUBNET Solutions Inc. has identified vulnerabilities in third-party components used in Substation Server.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33222	An issue in the component ATSZIO64.sys of ASUSTeK Computer Inc ASUS ATSZIO Driver v0.2.1.7 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	8.4	More Details
CVE-2024-33228	An issue in the component segwindrvx64.sys of Insyde Software Corp SEG Windows Driver v100.00.07.02 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	8.4	More Details
CVE-2024-4978	Justice AV Solutions Viewer Setup 8.3.7.250-1 contains a malicious binary when executed and is signed with an unexpected authenticode signature. A remote, privileged threat actor may exploit this vulnerability to execute of unauthorized PowerShell commands.	8.4	More Details
CVE-2024-35219	OpenAPI Generator allows generation of API client libraries (SDK generation), server stubs, documentation and configuration automatically given an OpenAPI Spec. Prior to version 7.6.0, attackers can exploit a path traversal vulnerability to read and delete files and folders from an arbitrary, writable directory as anyone can set the output folder when submitting the request via the `outputFolder` option. The issue was fixed in version 7.6.0 by removing the usage of the `outputFolder` option. No known workarounds are available.	8.3	More Details
CVE-2024-35553	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoMove_deal.php?mudi=add&nohrefStr=close.	8.3	More Details
CVE-2024-26139	OpenCTI is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. Due to lack of certain security controls on the profile edit functionality, an authenticated attacker with low privileges can gain administrative privileges on the web application.	8.3	More Details
CVE-2024-24947	A heap-based buffer overflow vulnerability exists in the Programming Software Connection CurrDir functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to denial of service. An attacker can send an unauthenticated packet to trigger these vulnerability.This CVE tracks the heap corruption that occurs at offset `0xb68c4` of version 1.2.10.9 of the P3-550E firmware, which occurs when a call to `memset` relies on an attacker-controlled length value and corrupts any trailing heap allocations.	8.2	More Details
CVE-2024-29072	A privilege escalation vulnerability exists in the Foxit Reader 2024.2.0.25138. The vulnerability occurs due to improper certification validation of the updater executable before executing it. A low privilege user can trigger the update action which can result in unexpected elevation of privilege.	8.2	More Details
CVE-2024-24946	A heap-based buffer overflow vulnerability exists in the Programming Software Connection CurrDir functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to denial of service. An attacker can send an unauthenticated packet to trigger these vulnerability.This CVE tracks the heap corruption that occurs at offset `0xb686c` of version 1.2.10.9 of the P3-550E firmware, which occurs when a call to `memset` relies on an attacker-controlled length value and corrupts any trailing heap allocations.	8.2	More Details
CVE-2024-35090	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in SysUreportFileMapper.xml.	8.2	More Details
CVE-2024-24957	Several out-of-bounds write vulnerabilities exist in the Programming Software Connection FileSystem API functionality of AutomationDirect P3-550E 1.2.10.9. Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.This CVE tracks the arbitrary null-byte write vulnerability located in firmware 1.2.10.9 of the P3-550E at offset `0xb6aa4`.	8.2	More Details
CVE-2024-36110	ansibleguy-webui is an open source WebUI for using Ansible. Multiple forms in versions < 0.0.21 allowed injection of HTML elements. These are returned to the user after executing job actions and thus evaluated by the browser. These issues have been addressed in version 0.0.21 (0.0.21.post2 on pypi). Users are advised to upgrade. There are no known workarounds for these issues.	8.2	More Details
CVE-2024-24959	Several out-of-bounds write vulnerabilities exist in the Programming Software Connection FileSystem API functionality of AutomationDirect P3-550E 1.2.10.9. Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.This CVE tracks the arbitrary null-byte write vulnerability located in firmware 1.2.10.9 of the P3-550E at offset `0xb6c18`.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24954	Several out-of-bounds write vulnerabilities exist in the Programming Software Connection FileSystem API functionality of AutomationDirect P3-550E 1.2.10.9. Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.This CVE tracks the arbitrary null-byte write vulnerability located in firmware 1.2.10.9 of the P3-550E at offset `0xb69c8`.	8.2	More Details
CVE-2024-24955	Several out-of-bounds write vulnerabilities exist in the Programming Software Connection FileSystem API functionality of AutomationDirect P3-550E 1.2.10.9. Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.This CVE tracks the arbitrary null-byte write vulnerability located in firmware 1.2.10.9 of the P3-550E at offset `0xb69fc`.	8.2	More Details
CVE-2024-24958	Several out-of-bounds write vulnerabilities exist in the Programming Software Connection FileSystem API functionality of AutomationDirect P3-550E 1.2.10.9. Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.This CVE tracks the arbitrary null-byte write vulnerability located in firmware 1.2.10.9 of the P3-550E at offset `0xb6bdc`.	8.2	More Details
CVE-2024-24956	Several out-of-bounds write vulnerabilities exist in the Programming Software Connection FileSystem API functionality of AutomationDirect P3-550E 1.2.10.9. Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.This CVE tracks the arbitrary null-byte write vulnerability located in firmware 1.2.10.9 of the P3-550E at offset `0xb6a38`.	8.2	More Details
CVE-2023-49600	An out-of-bounds write vulnerability exists in the PlyFile ply_cast_ascii functionality of libigl v2.5.0. A specially crafted .ply file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2023-46694	Vtenext 21.02 allows an authenticated attacker to upload arbitrary files, potentially enabling them to execute remote commands. This flaw exists due to the application's failure to enforce proper authentication controls when accessing the Ckeditor file manager functionality.	8.1	More Details
CVE-2024-33402	A SQL injection vulnerability in /model/approve_petty_cash.php in campcodes Complete Web-Based School Management System 1.0 allows attacker to execute arbitrary SQL commands via the id parameter.	8.1	More Details
CVE-2024-36428	OrangeHRM 3.3.3 allows admin/viewProjects sortOrder SQL injection.	8.1	More Details
CVE-2024-5085	The Hash Form – Drag & Drop Form Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.1.0 via deserialization of untrusted input in the 'process_entry' function. This makes it possible for unauthenticated attackers 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.	8.1	More Details
CVE-2024-0867	The Email Log plugin for WordPress is vulnerable to Unauthenticated Hook Injection in all versions up to, and including, 2.4.8 via the check_nonce function. This makes it possible for unauthenticated attackers to execute actions with hooks in WordPress under certain circumstances. The action the attacker wishes to execute needs to have a nonce check, and the nonce needs to be known to the attacker. Furthermore, the absence of a capability check is a requirement.	8.1	More Details
CVE-2024-5158	Type Confusion in V8 in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to potentially perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2024-29415	The ip package through 2.0.1 for Node.js might allow SSRF because some IP addresses (such as 127.1, 01200034567, 012.1.2.3, 000:0:0000::01, and ::fFFf:127.0.0.1) are improperly categorized as globally routable via isPublic. NOTE: this issue exists because of an incomplete fix for CVE-2023-42282.	8.1	More Details
CVE-2024-4471	The 140+ Widgets	Best Addons For Elementor – FREE for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 1.4.3.1 via deserialization of untrusted input in the 'export_content' function. This allows authenticated attackers, with contributor-level permissions and above, 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 to delete arbitrary files, retrieve sensitive data, or execute code. Thanks, Francesco	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43848	Incorrect access control in the firewall management function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote authenticated users to alter local firewall settings of the device as if they were the administrator via HTTP POST request.	8.0	More Details
CVE-2023-43844	Aten PE6208 2.3.228 and 2.4.232 have default credentials for the privileged web interface account. The user is not asked to change the credentials after first login. If not changed, attackers can log in to the web interface and gain administrator privileges.	8.0	More Details
CVE-2024-4835	A XSS condition exists within GitLab in versions 15.11 before 16.10.6, 16.11 before 16.11.3, and 17.0 before 17.0.1. By leveraging this condition, an attacker can craft a malicious page to exfiltrate sensitive user information.	8.0	More Details
CVE-2024-30280	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-52548	Huawei Matebook D16(Model: CREM-WXX9, BIOS: v2.26) Arbitrary Memory Corruption in SMI Handler of ThisiServicesSmm SMM module. This can be leveraged by a malicious OS attacker to corrupt arbitrary SMRAM memory and, in turn, lead to code execution in SMM	7.8	More Details
CVE-2023-52710	Huawei Matebook D16(Model: CREM-WXX9, BIOS: v2.26), As the communication buffer size hasn't been properly validated to be of the expected size, it can partially overlap with the beginning SMRAM.This can be leveraged by a malicious OS attacker to corrupt data structures stored at the beginning of SMRAM and can potentially lead to code execution in SMM.	7.8	More Details
CVE-2023-52711	Various Issues Due To Exposed SMI Handler in AmdPspP2CmboxV2. The first issue can be leveraged to bypass the protections that have been put in place by previous UEFI phases to prevent direct access to the SPI flash. The second issue can be used to both leak and corrupt SMM memory thus potentially leading code execution in SMM	7.8	More Details
CVE-2023-52712	Various Issues Due To Exposed SMI Handler in AmdPspP2CmboxV2. The first issue can be leveraged to bypass the protections that have been put in place by previous UEFI phases to prevent direct access to the SPI flash. The second issue can be used to both leak and corrupt SMM memory, thus potentially leading code execution in SMM	7.8	More Details
CVE-2023-52547	Huawei Matebook D16(Model: CREM-WXX9, BIOS: v2.26. Memory Corruption in SMI Handler of HddPassword SMM Module. This can be leveraged by a malicious OS attacker to corrupt data structures stored at the beginning of SMRAM and can potentially lead to code execution in SMM.	7.8	More Details
CVE-2024-33221	An issue in the component AsusBSItf.sys of ASUSTeK Computer Inc ASUS BIOS Flash Driver v3.2.12.0 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	7.8	More Details
CVE-2021-47571	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8192e: Fix use after free in _rtl92e_pci_disconnect() The free_rtllib() function frees the "dev" pointer so there is use after free on the next line. Re-arrange things to avoid that.	7.8	More Details
CVE-2024-30279	Acrobat Reader versions 20.005.30574, 24.002.20736 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-2021-47541	In the Linux kernel, the following vulnerability has been resolved: net/mlx4_en: Fix an use-after-free bug in mlx4_en_try_alloc_resources() In mlx4_en_try_alloc_resources(), mlx4_en_copy_priv() is called and tmp->tx_cq will be freed on the error path of mlx4_en_copy_priv(). After that mlx4_en_alloc_resources() is called and there is a dereference of &tmp->tx_cq[t][i] in mlx4_en_alloc_resources(), which could lead to a use after free problem on failure of mlx4_en_copy_priv(). Fix this bug by adding a check of mlx4_en_copy_priv() 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_MLX4_EN=m show no new warnings, and our static analyzer no longer warns about this code.	7.8	More Details
CVE-2021-47525	In the Linux kernel, the following vulnerability has been resolved: serial: liteuart: fix use-after-free and memleak on unbind Deregister the port when unbinding the driver to prevent it from being used after releasing the driver data and leaking memory allocated by serial core.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47521	In the Linux kernel, the following vulnerability has been resolved: can: sja1000: fix use after free in ems_pcmcia_add_card() If the last channel is not available then "dev" is freed. Fortunately, we can just use "pdev->irq" instead. Also we should check if at least one channel was set up.	7.8	More Details
CVE-2021-47520	In the Linux kernel, the following vulnerability has been resolved: can: pch_can: pch_can_rx_normal: fix use after free After calling netif_receive_skb(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is dereferenced just after the call netif_receive_skb(skb). Reordering the lines solves the issue.	7.8	More Details
CVE-2024-33218	An issue in the component AsUpIO64.sys of ASUSTeK Computer Inc ASUS USB 3.0 Boost Storage Driver 5.30.20.0 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	7.8	More Details
CVE-2023-35951	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF.cpp functionality of libigl v2.4.0. A specially-crafted .off file can lead to a buffer overflow. An attacker can arbitrary code execution to trigger these vulnerabilities.This vulnerability exists within the code responsible for parsing geometric vertices of an OFF file.	7.8	More Details
CVE-2024-33219	An issue in the component AsIO64.sys of ASUSTeK Computer Inc ASUS SABERTOOTH X99 Driver v1.0.1.0 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	7.8	More Details
CVE-2024-22181	An out-of-bounds write vulnerability exists in the readNODE functionality of libigl v2.5.0. A specially crafted .node file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2024-3969	XML External Entity injection vulnerability found in OpenText™ iManager 3.2.6.0200. This could lead to remote code execution by parsing untrusted XML payload	7.8	More Details
CVE-2024-24686	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF functionality of libigl v2.5.0. A specially crafted .off file can lead to stack-based buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the parsing of comments within the faces section of an `.off` file processed via the `readOFF` function.	7.8	More Details
CVE-2024-24685	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF functionality of libigl v2.5.0. A specially crafted .off file can lead to stack-based buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the parsing of comments within the vertex section of an `.off` file processed via the `readOFF` function.	7.8	More Details
CVE-2024-24684	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF functionality of libigl v2.5.0. A specially crafted .off file can lead to stack-based buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability concerns the header parsing occuring while processing an `.off` file via the `readOFF` function. We can see above that at [0] a stack-based buffer called `comment` is defined with an hardcoded size of `1000 bytes`. The call to `fscanf` at [1] is unsafe and if the first line of the header of the `.off` files is longer than 1000 bytes it will overflow the `header` buffer.	7.8	More Details
CVE-2024-4453	GStreamer EXIF Metadata Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GStreamer. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the parsing of EXIF metadata. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. . Was ZDI-CAN-23896.	7.8	More Details
CVE-2024-33225	An issue in the component RTKVHD64.sys of Realtek Semiconductor Corp Realtek(r) High Definition Audio Function Driver v6.0.9549.1 allows attackers to escalate privileges and execute arbitrary code via sending crafted IOCTL requests.	7.8	More Details
CVE-2024-34477	configureNFS in lib/common/functions.sh in FOG through 1.5.10 allows local users to gain privileges by mounting a crafted NFS share (because of no_root_squash and insecure). In order to exploit the vulnerability, someone needs to mount an NFS share in order to add an executable file as root. In addition, the SUID bit must be added to this file.	7.8	More Details
CVE-2023-35953	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF.cpp functionality of libigl v2.4.0. A specially-crafted .off file can lead to a buffer overflow. An attacker can arbitrary code execution to trigger these vulnerabilities.This vulnerability exists within the code responsible for parsing comments within the geometric vertices section within an OFF file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35952	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF.cpp functionality of libigl v2.4.0. A specially-crafted .off file can lead to a buffer overflow. An attacker can arbitrary code execution to trigger these vulnerabilities.This vulnerability exists within the code responsible for parsing comments within the geometric faces section within an OFF file.	7.8	More Details
CVE-2023-35950	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF.cpp functionality of libigl v2.4.0. A specially-crafted .off file can lead to a buffer overflow. An attacker can arbitrary code execution to trigger these vulnerabilities.This vulnerability exists within the code responsible for parsing the header of an OFF file.	7.8	More Details
CVE-2023-35949	Multiple stack-based buffer overflow vulnerabilities exist in the readOFF.cpp functionality of libigl v2.4.0. A specially-crafted .off file can lead to a buffer overflow. An attacker can arbitrary code execution to trigger these vulnerabilities.This vulnerability exists within the code responsible for parsing geometric faces of an OFF file.	7.8	More Details
CVE-2024-5202	Arbitrary File Read in OpenText Dimensions RM allows authenticated users to read files stored on the server via webservices	7.7	More Details
CVE-2024-35224	OpenProject is the leading open source project management software. OpenProject utilizes `tablesorter` inside of the Cost Report feature. This dependency, when misconfigured, can lead to Stored XSS via `{icon}` substitution in table header values. This attack requires the permissions "Edit work packages" as well as "Add attachments". A project admin could attempt to escalate their privileges by sending this XSS to a System Admin. Otherwise, if a full System Admin is required, then this attack is significantly less impactful. By utilizing a ticket's attachment, you can store javascript in the application itself and bypass the application's CSP policy to achieve Stored XSS. This vulnerability has been patched in version(s) 14.1.0, 14.0.2 and 13.4.2.	7.6	More Details
CVE-2024-36109	CoCalc is web-based software that enables collaboration in research, teaching, and scientific publishing. In affected versions the markdown parser allows `<script>` tags to be included which execute when published. This issue has been addressed in commit `419862a9c9879c`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.6	More Details
CVE-2023-30311	An issue discovered in H3C Magic R365 and H3C Magic R100 routers allows attackers to hijack TCP sessions which could lead to a denial of service.	7.5	More Details
CVE-2023-30313	An issue discovered in Wavlink QUANTUM D2G routers allows attackers to hijack TCP sessions which could lead to a denial of service.	7.5	More Details
CVE-2024-35618	PingCAP TiDB v7.5.1 was discovered to contain a NULL pointer dereference via the component SortedRowContainer.	7.5	More Details
CVE-2024-4388	This does not validate a path generated with user input when downloading files, allowing unauthenticated user to download arbitrary files from the server	7.5	More Details
CVE-2024-35341	Certain Anpviz products allow unauthenticated users to download the running configuration of the device via a HTTP GET request to /ConfigFile.ini or /config.xml URIs. This configuration file contains usernames and encrypted passwords (encrypted with a hardcoded key common to all devices). This affects IPC-D250, IPC-D260, IPC-B850, IPC-D850, IPC-D350, IPC-D3150, IPC-D4250, IPC-D380, IPC-D880, IPC-D280, IPC-D3180, MC800N, YM500L, YM800N_N2, YMF50B, YM800SV2, YM500L8, and YM200E10 firmware v3.2.2.2 and lower and possibly more vendors/models of IP camera.	7.5	More Details
CVE-2023-30310	An issue discovered in Comfast Comfast CF-616AC routers allows attackers to hijack TCP sessions which could lead to a denial of service.	7.5	More Details
CVE-2023-30305	An issue discovered in Linksys E5600 routers allows attackers to hijack TCP sessions which could lead to a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35237	MIT IdentiBot is an open-source Discord bot written in Node.js that verifies individuals' affiliations with MIT, grants them roles in a Discord server, and stores information about them in a database backend. A vulnerability that exists prior to commit 48e3e5e7ead6777fa75d57c7711c8e55b501c24e impacts all users who have performed verification with an instance of MIT IdentiBot that meets the following conditions: The instance of IdentiBot is tied to a "public" Discord application—i.e., users other than the API access registrant can add it to servers; *and* the instance has not yet been patched. In affected versions, IdentiBot does not check that a server is authorized before allowing members to execute slash and user commands in that server. As a result, any user can join IdentiBot to their server and then use commands (e.g., `/kerbid`) to reveal the full name and other information about a Discord user who has verified their affiliation with MIT using IdentiBot. The latest version of MIT IdentiBot contains a patch for this vulnerability (implemented in commit 48e3e5e7ead6777fa75d57c7711c8e55b501c24e). There is no way to prevent exploitation of the vulnerability without the patch. To prevent exploitation of the vulnerability, all vulnerable instances of IdentiBot should be taken offline until they have been updated.	7.5	More Details
CVE-2024-36426	In TARGIT Decision Suite 23.2.15007.0 before Autumn 2023, the session token is part of the URL and may be sent in a cleartext HTTP session.	7.5	More Details
CVE-2024-35081	LuckyFrameWeb v3.5.2 was discovered to contain an arbitrary file deletion vulnerability via the fileName parameter in the fileDownload method.	7.5	More Details
CVE-2024-4157	The Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 5.1.15 via deserialization of untrusted input in the extractDynamicValues function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. 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. Successful exploitation requires the attacker to have "View Form" and "Manage Form" permissions, which must be explicitly set by an administrator. However, this requirement can be bypassed when this vulnerability is chained with CVE-2024-2771.	7.5	More Details
CVE-2024-22641	TCPDF version 6.6.5 and before is vulnerable to ReDoS (Regular Expression Denial of Service) if parsing an untrusted SVG file.	7.5	More Details
CVE-2024-3657	A flaw was found in 389-ds-base. A specially-crafted LDAP query can potentially cause a failure on the directory server, leading to a denial of service	7.5	More Details
CVE-2024-24851	A heap-based buffer overflow vulnerability exists in the Programming Software Connection FiBurn functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to a buffer overflow. An attacker can send an unauthenticated packet to trigger this vulnerability.	7.5	More Details
CVE-2024-2038	The Visual Website Collaboration, Feedback & Project Management – Atarim plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 3.22.6. This is due to the use of hardcoded credentials to authenticate all the incoming API requests. This makes it possible for unauthenticated attackers to modify plugin settings, delete posts, modify post titles, and upload images.	7.5	More Details
CVE-2024-32988	'OfferBox' App for Android versions 2.0.0 to 2.3.17 and 'OfferBox' App for iOS versions 2.1.7 to 2.6.14 use a hard-coded secret key for JWT. Secret key for JWT may be retrieved if the application binary is reverse-engineered.	7.5	More Details
CVE-2021-47486	In the Linux kernel, the following vulnerability has been resolved: riscv, bpf: Fix potential NULL dereference The bpf_jit_binary_free() function requires a non-NULL argument. When the RISC-V BPF JIT fails to converge in NR_JIT_ITERATIONS steps, jit_data->header will be NULL, which triggers a NULL dereference. Avoid this by checking the argument, prior calling the function.	7.5	More Details
CVE-2024-23315	A read-what-where vulnerability exists in the Programming Software Connection IMM 01A1 Memory Read functionality of AutomationDirect P3-550E 1.2.10.9. A specially crafted network packet can lead to a disclosure of sensitive information. An attacker can send an unauthenticated packet to trigger this vulnerability.	7.5	More Details
CVE-2024-36054	Hw64.sys in Marvin Test HW.exe before 5.0.5.0 allows unprivileged user-mode processes to arbitrarily read kernel memory (and consequently gain all privileges) via IOCTL 0x9c4064b8 (via MmMapIoSpace) and IOCTL 0x9c406490 (via ZwMapViewOfSection).	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27264	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 284563.	7.4	More Details
CVE-2024-34454	Nintendo Wii U OS 5.5.5 allows man-in-the-middle attackers to forge SSL certificates as though they came from a Root CA, because there is a secondary verification mechanism that only checks whether a CA is known and ignores the CA details and signature (and because * is accepted as a Common Name).	7.4	More Details
CVE-2021-47464	In the Linux kernel, the following vulnerability has been resolved: audit: fix possible null-pointer dereference in audit_filter_rules Fix possible null-pointer dereference in audit_filter_rules. audit_filter_rules() error: we previously assumed 'ctx' could be null	7.4	More Details
CVE-2024-5357	A vulnerability has been found in PHPGurukul Zoo Management System 2.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266269 was assigned to this vulnerability.	7.3	More Details
CVE-2024-5362	A vulnerability classified as critical has been found in SourceCodester Online Hospital Management System 1.0. Affected is an unknown function of the file departmentDoctor.php. The manipulation of the argument deptid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-266274 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-30312	An issue discovered in OpenWrt 18.06, 19.07, 21.02, 22.03, and beyond allows off-path attackers to hijack TCP sessions, which could lead to a denial of service, impersonating the client to the server (e.g., for access to files over FTP), and impersonating the server to the client (e.g., to deliver false information from a finance website). This occurs because nf_conntrack_tcp_no_window_check is true by default.	7.3	More Details
CVE-2024-34928	A SQL injection vulnerability in /model/update_subject_routing.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the grade parameter.	7.3	More Details
CVE-2024-5377	A vulnerability was found in SourceCodester Vehicle Management System 1.0. It has been classified as critical. This affects an unknown part of the file /newvehicle.php. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266289 was assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47441	In the Linux kernel, the following vulnerability has been resolved: mlxsw: thermal: Fix out-of-bounds memory accesses Currently, mlxsw allows cooling states to be set above the maximum cooling state supported by the driver: # cat /sys/class/thermal/thermal_zone2/cdev0/type mlxsw_fan # cat /sys/class/thermal/thermal_zone2/cdev0/max_state 10 # echo 18 > /sys/class/thermal/thermal_zone2/cdev0/cur_state # echo $? 0 This results in out-of-bounds memory accesses when thermal state transition statistics are enabled (CONFIG_THERMAL_STATISTICS=y), as the transition table is accessed with a too large index (state) [1]. According to the thermal maintainer, it is the responsibility of the driver to reject such operations [2]. Therefore, return an error when the state to be set exceeds the maximum cooling state supported by the driver. To avoid dead code, as suggested by the thermal maintainer [3], partially revert commit a421ce088ac8 ("mlxsw: core: Extend cooling device with cooling levels") that tried to interpret these invalid cooling states (above the maximum) in a special way. The cooling levels array is not removed in order to prevent the fans going below 20% PWM, which would cause them to get stuck at 0% PWM. [1] BUG: KASAN: slab-out-of-bounds in thermal_cooling_device_stats_update+0x271/0x290 Read of size 4 at addr ffff8881052f7bf8 by task kworker/0:0/5 CPU: 0 PID: 5 Comm: kworker/0:0 Not tainted 5.15.0-rc3-custom-45935-gce1adf704b14 #122 Hardware name: Mellanox Technologies Ltd. "MSN2410-CB2FO"/"SA000874", BIOS 4.6.5 03/08/2016 Workqueue: events_freezable_power_ thermal_zone_device_check Call Trace: dump_stack_lvl+0x8b/0xb3 print_address_description.constprop.0+0x1f/0x140 kasan_report.cold+0x7f/0x11b thermal_cooling_device_stats_update+0x271/0x290 __thermal_cdev_update+0x15e/0x4e0 thermal_cdev_update+0x9f/0xe0 step_wise_throttle+0x770/0xee0 thermal_zone_device_update+0x3f6/0xdf0 process_one_work+0xa42/0x1770 worker_thread+0x62f/0x13e0 kthread+0x3ee/0x4e0 ret_from_fork+0x1f/0x30 Allocated by task 1: kasan_save_stack+0x1b/0x40 __kasan_kmalloc+0x7c/0x90 thermal_cooling_device_setup_sysfs+0x153/0x2c0 __thermal_cooling_device_register.part.0+0x25b/0x9c0 thermal_cooling_device_register+0xb3/0x100 mlxsw_thermal_init+0x5c5/0x7e0 __mlxsw_core_bus_device_register+0xcb3/0x19c0 mlxsw_core_bus_device_register+0x56/0xb0 mlxsw_pci_probe+0x54f/0x710 local_pci_probe+0xc6/0x170 pci_device_probe+0x2b2/0x4d0 really_probe+0x293/0xd10 __driver_probe_device+0x2af/0x440 driver_probe_device+0x51/0x1e0 __driver_attach+0x21b/0x530 bus_for_each_dev+0x14c/0x1d0 bus_add_driver+0x3ac/0x650 driver_register+0x241/0x3d0 mlxsw_sp_module_init+0xa2/0x174 do_one_initcall+0xee/0x5f0 kernel_init_freeable+0x45a/0x4de kernel_init+0x1f/0x210 ret_from_fork+0x1f/0x30 The buggy address belongs to the object at ffff8881052f7800 which belongs to the cache kmalloc-1k of size 1024 The buggy address is located 1016 bytes inside of 1024-byte region [ffff8881052f7800, ffff8881052f7c00) The buggy address belongs to the page: page:0000000052355272 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1052f0 head:0000000052355272 order:3 compound_mapcount:0 compound_pincount:0 flags: 0x200000000010200(slablheadlnode=0lzone=2) raw: 0200000000010200 ffffea0005034800 0000000300000003 ffff888100041dc0 raw: 0000000000000000 0000000000100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8881052f7a80: 00 00 00 00 00 00 04 fc fc fc fc fc fc fc fc ffff8881052f7b00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc >ffff8881052f7b80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ^ ffff8881052f7c00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffff8881052f7c80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [2] https://lore.kernel.org/linux-pm/9aca37cb-1629-5c67- ---truncated---	7.3	More Details
CVE-2023-43843	Incorrect access control in the account management function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote authenticated users to read user and administrator accounts passwords via HTTP GET request.	7.3	More Details
CVE-2024-35226	Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. In affected versions template authors could inject php code by choosing a malicious file name for an extends-tag. Sites that cannot fully trust template authors should update asap. All users are advised to update. There is no patch for users on the v3 branch. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2023-43842	Incorrect access control in the account management function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote authenticated users to alter user and administrator accounts credentials via HTTP POST request.	7.3	More Details
CVE-2024-5384	A vulnerability classified as critical was found in SourceCodester Facebook News Feed Like 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument page leads to sql injection. The attack can be initiated remotely. VDB-266302 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-33471	An issue in the Sensor Settings of AVTECH Room Alert 4E v4.4.0 allows attackers to gain access to SMTP credentials in plaintext via a crafted AJAX request. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5399	Openfind Mail2000 does not properly filter parameters of specific API. Remote attackers with administrative privileges can exploit this vulnerability to execute arbitrary system commands on the remote server.	7.2	More Details
CVE-2022-48681	Some Huawei smart speakers have a memory overflow vulnerability. Successful exploitation of this vulnerability may cause certain functions to fail.	7.2	More Details
CVE-2024-4455	The YITH WooCommerce Ajax Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'item' parameter in versions up to, and including, 2.4.0 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-2024-5403	ASKEY 5G NR Small Cell fails to properly filter user input for certain functionality, allowing remote attackers with administrator privilege to execute arbitrary system commands on the remote server.	7.2	More Details
CVE-2024-4262	The Piotnet Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 2.4.28 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.	7.2	More Details
CVE-2024-4347	The WP Fastest Cache plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.2.6 via the specificDeleteCache function. This makes it possible for authenticated attackers to delete arbitrary files on the server, which can include wp-config.php files of the affected site or other sites in a shared hosting environment.	7.2	More Details
CVE-2024-30056	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	7.1	More Details
CVE-2023-49575	A vulnerability has been discovered in VX Search Enterprise affecting version 10.2.14 that could allow an attacker to execute persistent XSS through /setup_smtp in smtp_server, smtp_user, smtp_password and smtp_email_address parameters. This vulnerability could allow an attacker to store malicious JavaScript payloads on the system to be triggered when the page loads.	7.1	More Details
CVE-2023-49572	A vulnerability has been discovered in VX Search Enterprise affecting version 10.2.14 that could allow an attacker to execute persistent XSS through /setup_odbc in odbc_data_source, odbc_user and odbc_password parameters. This vulnerability could allow an attacker to store malicious JavaScript payloads on the system to be triggered when the page loads.	7.1	More Details
CVE-2023-49573	A vulnerability has been discovered in VX Search Enterprise affecting version 10.2.14 that could allow an attacker to execute persistent XSS through /add_command_action in action_value. This vulnerability could allow an attacker to store malicious JavaScript payloads on the system to be triggered when the page loads.	7.1	More Details
CVE-2023-49574	A vulnerability has been discovered in VX Search Enterprise affecting version 10.2.14 that could allow an attacker to execute persistent XSS through /add_job in job_name. This vulnerability could allow an attacker to store malicious JavaScript payloads on the system to be triggered when the page loads.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47465	In the Linux kernel, the following vulnerability has been resolved: KVM: PPC: Book3S HV: Fix stack handling in idle_kvm_start_guest() In commit 10d91611f426 ("powerpc/64s: Reimplement book3s idle code in C") kvm_start_guest() became idle_kvm_start_guest(). The old code allocated a stack frame on the emergency stack, but didn't use the frame to store anything, and also didn't store anything in its caller's frame. idle_kvm_start_guest() on the other hand is written more like a normal C function, it creates a frame on entry, and also stores CR/LR into its callers frame (per the ABI). The problem is that there is no caller frame on the emergency stack. The emergency stack for a given CPU is allocated with: paca_ptrs[i]->emergency_sp = alloc_stack(limit, i) + THREAD_SIZE; So emergency_sp actually points to the first address above the emergency stack allocation for a given CPU, we must not store above it without first decrementing it to create a frame. This is different to the regular kernel stack, paca->kstack, which is initialised to point at an initial frame that is ready to use. idle_kvm_start_guest() stores the backchain, CR and LR all of which write outside the allocation for the emergency stack. It then creates a stack frame and saves the non-volatile registers. Unfortunately the frame it creates is not large enough to fit the non-volatiles, and so the saving of the non-volatile registers also writes outside the emergency stack allocation. The end result is that we corrupt whatever is at 0-24 bytes, and 112-248 bytes above the emergency stack allocation. In practice this has gone unnoticed because the memory immediately above the emergency stack happens to be used for other stack allocations, either another CPUs mc_emergency_sp or an IRQ stack. See the order of calls to irqstack_early_init() and emergency_stack_init(). The low addresses of another stack are the top of that stack, and so are only used if that stack is under extreme pressue, which essentially never happens in practice - and if it did there's a high likelyhood we'd crash due to that stack overflowing. Still, we shouldn't be corrupting someone else's stack, and it is purely luck that we aren't corrupting something else. To fix it we save CR/LR into the caller's frame using the existing r1 on entry, we then create a SWITCH_FRAME_SIZE frame (which has space for pt_regs) on the emergency stack with the backchain pointing to the existing stack, and then finally we switch to the new frame on the emergency stack.	7.1	More Details
CVE-2024-5413	A vulnerability have been discovered in PhpMyBackupPro affecting version 2.3 that could allow an attacker to execute XSS through /phpmybackuppro/scheduled.php, all parameters. This vulnerabilities could allow an attacker to create a specially crafted URL and send it to a victim to retrieve their session details.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47449	In the Linux kernel, the following vulnerability has been resolved: ice: fix locking for Tx timestamp tracking flush Commit 4dd0d5c33c3e ("ice: add lock around Tx timestamp tracker flush") added a lock around the Tx timestamp tracker flow which is used to cleanup any left over SKBs and prepare for device removal. This lock is problematic because it is being held around a call to ice_clear_phy_tstamp. The clear function takes a mutex to send a PHY write command to firmware. This could lead to a deadlock if the mutex actually sleeps, and causes the following warning on a kernel with preemption debugging enabled: [715.419426] BUG: sleeping function called from invalid context at kernel/locking/mutex.c:573 [715.427900] in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 3100, name: rmmod [715.435652] INFO: lockdep is turned off. [715.439591] Preemption disabled at: [715.439594] [<0000000000000000>] 0x0 [715.446678] CPU: 52 PID: 3100 Comm: rmmod Tainted: G W OE 5.15.0-rc4+ #42 bdd7ec3018e725f159ca0d372ce8c2c0e784891c [715.458058] Hardware name: Intel Corporation S2600STQ/S2600STQ, BIOS SE5C620.86B.02.01.0010.010620200716 01/06/2020 [715.468483] Call Trace: [715.470940] dump_stack_lvl+0x6a/0x9a [715.474613] ___might_sleep.cold+0x224/0x26a [715.478895] __mutex_lock+0xb3/0x1440 [715.482569] ? stack_depot_save+0x378/0x500 [715.486763] ? ice_sq_send_cmd+0x78/0x14c0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.494979] ? kfree+0xc1/0x520 [715.498128] ? mutex_lock_io_nested+0x12a0/0x12a0 [715.502837] ? kasan_set_free_info+0x20/0x30 [715.507110] ? __kasan_slab_free+0x10b/0x140 [715.511385] ? slab_free_freelist_hook+0xc7/0x220 [715.516092] ? kfree+0xc1/0x520 [715.519235] ? ice_deinit_lag+0x16c/0x220 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.527359] ? ice_remove+0x1cf/0x6a0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.535133] ? pci_device_remove+0xab/0x1d0 [715.539318] ? __device_release_driver+0x35b/0x690 [715.544110] ? driver_detach+0x214/0x2f0 [715.548035] ? bus_remove_driver+0x11d/0x2f0 [715.552309] ? pci_unregister_driver+0x26/0x250 [715.556840] ? ice_module_exit+0xc/0x2f [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.564799] ? __do_sys_delete_module.constprop.0+0x2d8/0x4e0 [715.570554] ? do_syscall_64+0x3b/0x90 [715.574303] ? entry_SYSCALL_64_after_hwframe+0x44/0xae [715.579529] ? start_flush_work+0x542/0x8f0 [715.583719] ? ice_sq_send_cmd+0x78/0x14c0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.591923] ice_sq_send_cmd+0x78/0x14c0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.599960] ? wait_for_completion_io+0x250/0x250 [715.604662] ? lock_acquire+0x196/0x200 [715.608504] ? do_raw_spin_trylock+0xa5/0x160 [715.612864] ice_sbq_rw_reg+0x1e6/0x2f0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.620813] ? ice_reset+0x130/0x130 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.628497] ? __debug_check_no_obj_freed+0x1e8/0x3c0 [715.633550] ? trace_hardirqs_on+0x1c/0x130 [715.637748] ice_write_phy_reg_e810+0x70/0xf0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.646220] ? do_raw_spin_trylock+0xa5/0x160 [715.650581] ? ice_ptp_release+0x910/0x910 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.658797] ? ice_ptp_release+0x255/0x910 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.667013] ice_clear_phy_tstamp+0x2c/0x110 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.675403] ice_ptp_release+0x408/0x910 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.683440] ice_remove+0x560/0x6a0 [ice 9a7e1ec00971c89ecd3fe0d4dc7da2b3786a421d] [715.691037] ? _raw_spin_unlock_irqrestore+0x46/0x73 [715.696005] pci_device_remove+0xab/0x1d0 [715.700018] __device_release_driver+0x35b/0x690 [715.704637] driver_detach+0x214/0x2f0 [715.708389] bus_remove_driver+0x11d/0x2f0 [715.712489] pci_unregister_driver+0x26/0x250 [71 ---truncated---	7.1	More Details
CVE-2024-30165	Amazon AWS Client VPN before 3.9.1 on macOS has a buffer overflow that could potentially allow a local actor to execute arbitrary commands with elevated permissions, a different vulnerability than CVE-2024-30164.	7.1	More Details
CVE-2024-5408	Vulnerability in RhinOS 3.0-1190 consisting of an XSS through the "search" parameter of /portal/search.htm. This vulnerability could allow a remote attacker to steal details of a victim's user session by submitting a specially crafted URL.	7.1	More Details
CVE-2024-5415	A vulnerability have been discovered in PhpMyBackupPro affecting version 2.3 that could allow an attacker to execute XSS through /phpmybackuppro/backup.php, 'comments' and 'db' parameters. This vulnerabilities could allow an attacker to create a specially crafted URL and send it to a victim to retrieve their session details.	7.1	More Details
CVE-2024-4531	The Business Card WordPress plugin through 1.0.0 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions such as editing cards via CSRF attacks	7.1	More Details
CVE-2024-5409	RhinOS 3.0-1190 is vulnerable to an XSS via the "tamper" parameter in /admin/lib/phpthumb/phpthumb.php. An attacker could create a malicious URL and send it to a victim to obtain their session details.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5414	A vulnerability have been discovered in PhpMyBackupPro affecting version 2.3 that could allow an attacker to execute XSS through /phpmybackuppro/get_file.php, 'view' parameter. This vulnerabilities could allow an attacker to create a specially crafted URL and send it to a victim to retrieve their session details.	7.1	More Details
CVE-2024-36013	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix slab-use-after-free in l2cap_connect() Extend a critical section to prevent chan from early freeing. Also make the l2cap_connect() return type void. Nothing is using the returned value but it is ugly to return a potentially freed pointer. Making it void will help with backports because earlier kernels did use the return value. Now the compile will break for kernels where this patch is not a complete fix. Call stack summary: [use] l2cap_bredr_sig_cmd l2cap_connect ┌ mutex_lock(&conn->chan_lock); | chan = pchan->ops->new_connection(pchan); <- alloc chan | __l2cap_chan_add(conn, chan); | l2cap_chan_hold(chan); | list_add(&chan->list, &conn->chan_l); ... (1) └ mutex_unlock(&conn->chan_lock); chan->conf_state ... (4) <- use after free [free] l2cap_conn_del ┌ mutex_lock(&conn->chan_lock); | foreach chan in conn->chan_l: ... (2) | l2cap_chan_put(chan); | l2cap_chan_destroy | kfree(chan) ... (3) <- chan freed └ mutex_unlock(&conn->chan_lock); == BUG: KASAN: slab-use-after-free in instrument_atomic_read include/linux/instrumented.h:68 [inline] BUG: KASAN: slab-use-after-free in _test_bit include/asm-generic/bitops/instrumented-non-atomic.h:141 [inline] BUG: KASAN: slab-use-after-free in l2cap_connect+0xa67/0x11a0 net/bluetooth/l2cap_core.c:4260 Read of size 8 at addr ffff88810bf040a0 by task kworker/u3:1/311	6.8	More Details
CVE-2024-5143	A user with device administrative privileges can change existing SMTP server settings on the device, without having to re-enter SMTP server credentials. By redirecting send-to-email traffic to the new server, the original SMTP server credentials may potentially be exposed.	6.8	More Details
CVE-2024-36361	Pug through 3.0.2 allows JavaScript code execution if an application accepts untrusted input for the name option of the compileClient, compileFileClient, or compileClientWithDependenciesTracked function. NOTE: these functions are for compiling Pug templates into JavaScript, and there would typically be no reason to allow untrusted callers.	6.8	More Details
CVE-2024-22026	A local privilege escalation vulnerability in EPMM before 12.1.0.0 allows an authenticated local user to bypass shell restriction and execute arbitrary commands on the appliance.	6.7	More Details
CVE-2024-30164	Amazon AWS Client VPN has a buffer overflow that could potentially allow a local actor to execute arbitrary commands with elevated permissions. This is resolved in 3.11.1 on Windows, 3.9.1 on macOS, and 3.12.1 on Linux. NOTE: although the macOS resolution is the same as for CVE-2024-30165, this vulnerability on macOS is not the same as CVE-2024-30165.	6.7	More Details
CVE-2024-32978	Kaminari is a paginator for web app frameworks and object relational mappings. A security vulnerability involving insecure file permissions has been identified in the Kaminari pagination library for Ruby on Rails, concerning insecure file permissions. This vulnerability is of moderate severity due to the potential for unauthorized write access to particular Ruby files managed by the library. Such access could lead to the alteration of application behavior or data integrity issues. Users of affected versions are advised to update to Kaminari version 0.16.2 or later, where file permissions have been adjusted to enhance security. If upgrading is not feasible immediately, review and adjust the file permissions for particular Ruby files in Kaminari to ensure they are only accessible by authorized user.	6.6	More Details
CVE-2024-31396	Code injection vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.12 and Ver.3.0.x series versions prior to Ver.3.0.32. If this vulnerability is exploited, a user with an administrator or higher privilege who can log in to the product may execute an arbitrary command on the server.	6.6	More Details
CVE-2024-36079	An issue was discovered in Vaultize 21.07.27. When uploading files, there is no check that the filename parameter is correct. As a result, a temporary file will be created outside the specified directory when the file is downloaded. To exploit this, an authenticated user would upload a file with an incorrect file name, and then download it.	6.5	More Details
CVE-2024-33849	ci solution CI-Out-of-Office Manager through 6.0.0.77 uses a Hard-coded Cryptographic Key.	6.5	More Details
CVE-2021-47551	In the Linux kernel, the following vulnerability has been resolved: drm/amd/amdkfd: Fix kernel panic when reset failed and been triggered again In SRIOV configuration, the reset may failed to bring asic back to normal but stop cpsch already been called, the start_cpsch will not be called since there is no resume in this case. When reset been triggered again, driver should avoid to do uninitialization again.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2874	An issue has been discovered in GitLab CE/EE affecting all versions before 16.10.6, version 16.11 before 16.11.3, and 17.0 before 17.0.1. A runner registered with a crafted description has the potential to disrupt the loading of targeted GitLab web resources.	6.5	More Details
CVE-2024-5165	In Eclipse Ditto versions 3.0.0 to 3.5.5, the user input of several input fields of the Eclipse Ditto Explorer User Interface https://eclipse.dev/ditto/user-interface.html was not properly neutralized and thus vulnerable to both Reflected and Stored XSS (Cross Site Scripting). Several inputs were not persisted at the backend of Eclipse Ditto, but only in local browser storage to save settings of "environments" of the UI and e.g. the last performed "search queries", resulting in a "Reflected XSS" vulnerability. However, several other inputs were persisted at the backend of Eclipse Ditto, leading to a "Stored XSS" vulnerability. Those mean that authenticated and authorized users at Eclipse Ditto can persist Things in Ditto which can - when being displayed by other users also being authorized to see those Things in the Eclipse Ditto UI - cause scripts to be executed in the browser of other users.	6.5	More Details
CVE-2024-4037	The WP Photo Album Plus plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 8.7.02.003. This is due to the plugin allowing unauthenticated users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	6.5	More Details
CVE-2023-43849	Incorrect access control in firmware upgrade function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote authenticated users to submit a firmware image via HTTP POST requests. This may result in DoS or remote code execution.	6.5	More Details
CVE-2024-36049	Aptos Wisal payroll accounting before 7.1.6 uses hardcoded credentials in the Windows client to fetch the complete list of usernames and passwords from the database server, using an unencrypted connection. This allows attackers in a machine-in-the-middle position read and write access to personally identifiable information (PII) and especially payroll data and the ability to impersonate legitimate users with respect to the audit log.	6.5	More Details
CVE-2024-22588	Kwik commit 745fd4e2 does not discard unused encryption keys.	6.5	More Details
CVE-2024-23580	HCL DRYiCE Optibot Reset Station is impacted by insecure encryption of One-Time Passwords (OTPs). This could allow an attacker with access to the database to recover some or all encrypted values.	6.5	More Details
CVE-2024-5166	An Insecure Direct Object Reference in Google Cloud's Looker allowed metadata exposure across authenticated Looker users sharing the same LookML model.	6.5	More Details
CVE-2024-23579	HCL DRYiCE Optibot Reset Station is impacted by insecure encryption of security questions. This could allow an attacker with access to the database to recover some or all encrypted values.	6.5	More Details
CVE-2023-30314	An issue discovered in 360 V6G, 360 T5G, 360 T6M, and 360 P1 routers allows attackers to hijack TCP sessions which could lead to a denial of service.	6.5	More Details
CVE-2024-31904	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.25 and 12.0.1.0 through 12.0.12.0 integration nodes could allow an authenticated user to cause a denial of service due to an uncaught exception. IBM X-Force ID: 289647.	6.5	More Details
CVE-2024-33802	A SQL injection vulnerability in /model/get_student_subject.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the index parameter.	6.5	More Details
CVE-2024-36472	In GNOME Shell through 45.7, a portal helper can be launched automatically (without user confirmation) based on network responses provided by an adversary (e.g., an adversary who controls the local Wi-Fi network), and subsequently loads untrusted JavaScript code, which may lead to resource consumption or other impacts depending on the JavaScript code's behavior.	6.5	More Details
CVE-2023-30308	An issue discovered in Ruijie EG210G-P, Ruijie EG105G-V2, Ruijie NBR, and Ruijie EG105G routers allows attackers to hijack TCP sessions which could lead to a denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28880	Path traversal vulnerability in MosP kintai kanri V4.6.6 and earlier allows a remote attacker who can log in to the product to obtain sensitive information of the product.	6.5	More Details
CVE-2024-35162	Path traversal vulnerability exists in Download Plugins and Themes from Dashboard versions prior to 1.8.6. If this vulnerability is exploited, a remote authenticated attacker with "switch_themes" privilege may obtain arbitrary files on the server.	6.5	More Details
CVE-2024-1815	The Spectra – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Gallery block in all versions up to, and including, 2.12.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-35475	A Cross-Site Request Forgery (CSRF) vulnerability was discovered in OpenKM Community Edition on or before version 6.3.12. The vulnerability exists in /admin/DatabaseQuery, which allows an attacker to manipulate a victim with administrative privileges to execute arbitrary SQL commands.	6.4	More Details
CVE-2024-5177	The Hash Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter within multiple widgets in all versions up to, and including, 1.3.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3718	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's widgets all versions up to, and including, 5.5.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3648	The ShareThis Share Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sharethis-inline-button' shortcode in all versions up to, and including, 2.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5025	The Memberpress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘arglist’ parameter in all versions up to, and including, 1.11.29 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-2024-4896	The WPB Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter in all versions up to, and including, 1.0.9 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-2024-1814	The Spectra – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Testimonial block in all versions up to, and including, 2.12.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4043	The WP Ultimate Post Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpupg-text' shortcode in all versions up to, and including, 3.9.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4362	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'siteorigin_widget' shortcode in all versions up to, and including, 1.60.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4706	The WordPress + Microsoft Office 365 / Azure AD	LOGIN plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'pintra' shortcode in all versions up to, and including, 27.2 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-2024-4366	The Spectra – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘block_id’ parameter in versions up to, and including, 2.13.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5060	The LottieFiles – JSON Based Animation Lottie & Bodymovin for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.10.9 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-2024-4485	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 ‘button_custom_attributes’ parameter in versions up to, and including, 5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2861	The ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ProfilePress User Panel widget in all versions up to, and including, 4.15.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1332	The Custom Fonts – Host Your Fonts Locally plugin for WordPress is vulnerable to Stored Cross-Site Scripting via svg file upload in all versions up to, and including, 2.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author level or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3997	The Prime Slider – Addons For Elementor (Revolution of a slider, Hero Slider, Ecommerce Slider) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Pagepiling widget in all versions up to, and including, 3.14.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4431	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 1.3.7.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4532	The Business Card WordPress plugin through 1.0.0 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions such as deleting cards via CSRF attacks	6.4	More Details
CVE-2024-4980	The WPKoi Templates for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'id', 'mixColor', 'backgroundColor', 'saveInCookies', and 'autoMatchOsTheme' parameters in all versions up to, and including, 2.5.9 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-2024-3611	The Toolbar Extras for Elementor & More – WordPress Admin Bar Enhanced plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tbex-version' shortcode in all versions up to, and including, 1.4.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3066	The Elegant 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, 1.0.8 due to insufficient input sanitization and output escaping on user supplied tag 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-2024-2451	Improper fingerprint validation in the TeamViewer Client (Full & Host) prior Version 15.54 for Windows and macOS allows an attacker with administrative user rights to further elevate privileges via executable sideloading.	6.4	More Details
CVE-2024-4971	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 4.2.6.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.4	More Details
CVE-2024-5092	The Elegant Addons for elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Switcher, Slider, and Iconbox widgets in all versions up to, and including, 1.0.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3198	The WP Font Awesome Share Icons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpfai_social' shortcode in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2163	The Ninja Beaver Add-ons for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 2.4.5 due to insufficient input sanitization and output escaping on user supplied attributes such as urls. 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-2024-5205	The Videojs HTML5 Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's videojs_video shortcode in all versions up to, and including, 1.1.11 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-2024-2618	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the size attribute in all versions up to, and including, 1.6.26 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2784	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Hover Card widget in all versions up to, and including, 5.5.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3666	The Opal Estate Pro – Property Management and Submission plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the agent latitude and longitude parameters in all versions up to, and including, 1.7.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor 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-2024-3671	The Print-O-Matic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'print-me' shortcode in all versions up to, and including, 2.1.10 due to insufficient input sanitization and output escaping on user supplied attributes such as 'tag'. 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-2024-3557	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpgmza shortcode in all versions up to, and including, 9.0.36 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1134	The SEOPress – On-site SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the SEO title and description parameters as well as others in all versions up to, and including, 7.5.2.1 due to insufficient input sanitization and output escaping. This makes it possible for attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3926	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom_attributes value in widgets in all versions up to, and including, 5.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4045	The Popup Builder by OptinMonster – WordPress Popups for Optins, Email Newsletters and Lead Generation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘campaign_id’ parameter in versions up to, and including, 2.16.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5218	The Reviews and Rating – Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file upload feature in all versions up to, and including, 5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3201	The WP DSGVO Tools (GDPR) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'pp_link' shortcode in all versions up to, and including, 3.1.32 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-2024-4486	The Awesome Contact Form7 for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'AEP Contact Form 7' widget in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4783	The jQuery T(-) Countdown Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's tminus shortcode in all versions up to, and including, 2.3.25 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-2024-5229	The Primary Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Pricing Table widget in all versions up to, and including, 1.5.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5220	The ND Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's upload feature in all versions up to, and including, 7.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4484	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 ‘xai_username’ parameter in versions up to, and including, 5.5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4365	The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘add_iframe_url_as_param_direct’ parameter in versions up to, and including, 2024.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions 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-2024-4575	The LayerSlider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ls_search_form shortcode in version 7.11.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4378	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's menu and shape widgets in all versions up to, and including, 4.10.30 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-2024-33804	A SQL injection vulnerability in /model/get_subject.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	6.3	More Details
CVE-2024-5391	A vulnerability has been found in itsourcecode Online Student Enrollment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file listofsubject.php. The manipulation of the argument subjcode leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266305 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5406	A vulnerability had been discovered in WinNMP 19.02 consisting of an XSS attack via index page in from, subject, text and hash parameters. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their session details.	6.3	More Details
CVE-2024-28061	An issue was discovered in Apiris Kafeo 6.4.4. It permits a bypass, of the protection in place, to access to the data stored in the embedded database file.	6.3	More Details
CVE-2024-5312	PHP Server Monitor, version 3.2.0, is vulnerable to an XSS via the /phpservermon-3.2.0/vendor/phpmailer/phpmailer/test_script/index.php page in all visible parameters. An attacker could create a specially crafted URL, send it to a victim and retrieve their session details.	6.3	More Details
CVE-2024-5392	A vulnerability was found in itsourcecode Online Student Enrollment System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file editSubject.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. VDB-266306 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5381	A vulnerability classified as critical was found in itsourcecode Student Information Management System 1.0. Affected by this vulnerability is an unknown functionality of the file view.php. The manipulation of the argument studentId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266293 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5393	A vulnerability was found in itsourcecode Online Student Enrollment System 1.0. It has been classified as critical. This affects an unknown part of the file listofcourse.php. The manipulation of the argument idno leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266307.	6.3	More Details
CVE-2024-5394	A vulnerability was found in itsourcecode Online Student Enrollment System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file newDept.php. The manipulation of the argument deptname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266308.	6.3	More Details
CVE-2024-5366	A vulnerability has been found in SourceCodester Best House Rental Management System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file edit-cate.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-266278 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5365	A vulnerability, which was classified as critical, was found in SourceCodester Best House Rental Management System up to 1.0. This affects an unknown part of the file manage_payment.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266277 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5364	A vulnerability, which was classified as critical, has been found in SourceCodester Best House Rental Management System up to 1.0. Affected by this issue is some unknown functionality of the file manage_tenant.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. The identifier of this vulnerability is VDB-266276.	6.3	More Details
CVE-2024-5363	A vulnerability classified as critical was found in SourceCodester Best House Rental Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266275.	6.3	More Details
CVE-2024-5395	A vulnerability was found in itsourcecode Online Student Enrollment System 1.0. It has been rated as critical. This issue affects some unknown processing of the file listofinstructor.php. The manipulation of the argument FullName leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266309 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5361	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been rated as critical. This issue affects some unknown processing of the file /admin/normal-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266273 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5360	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/foreigner-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266272.	6.3	More Details
CVE-2024-5359	A vulnerability was found in PHPGurukul Zoo Management System 2.1. It has been classified as critical. This affects an unknown part of the file /admin/foreigner-search.php. The manipulation of the argument searchdata leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266271.	6.3	More Details
CVE-2024-5358	A vulnerability was found in PHPGurukul Zoo Management System 2.1 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/normal-search.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-266270 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5396	A vulnerability classified as critical has been found in itsourcecode Online Student Enrollment System 1.0. Affected is an unknown function of the file newfaculty.php. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-266310 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5356	A vulnerability, which was classified as critical, was found in anji-plus AJ-Report up to 1.4.1. Affected is an unknown function of the file /dataSet/testTransform;swagger-ui. The manipulation of the argument dynSentence leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266268.	6.3	More Details
CVE-2024-5355	A vulnerability, which was classified as critical, has been found in anji-plus AJ-Report up to 1.4.1. This issue affects the function IGroovyHandler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266267.	6.3	More Details
CVE-2024-5353	A vulnerability classified as critical has been found in anji-plus AJ-Report up to 1.4.1. This affects the function decompress of the component ZIP File Handler. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266265 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5352	A vulnerability was found in anji-plus AJ-Report up to 1.4.1. It has been rated as critical. Affected by this issue is the function validationRules of the component com.anjiplus.template.gaea.business.modules.datasetparam.controller.DataSetParamController#verification. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266264.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5351	A vulnerability was found in anji-plus AJ-Report up to 1.4.1. It has been declared as critical. Affected by this vulnerability is the function getValueFromJs of the component Javascript Handler. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266263.	6.3	More Details
CVE-2024-5350	A vulnerability was found in anji-plus AJ-Report up to 1.4.1. It has been classified as critical. Affected is the function pageList of the file /pageList. The manipulation of the argument p leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-266262 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5397	A vulnerability classified as critical was found in itsourcecode Online Student Enrollment System 1.0. Affected by this vulnerability is an unknown functionality of the file instructorSubjects.php. The manipulation of the argument instructorId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266311.	6.3	More Details
CVE-2024-4530	The Business Card WordPress plugin through 1.0.0 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions such as editing card categories via CSRF attacks	6.3	More Details
CVE-2024-34852	F-logic DataCube3 v1.0 is affected by command injection due to improper string filtering at the command execution point in the ./admin/transceiver_schedule.php file. An unauthenticated remote attacker can exploit this vulnerability by sending a file name containing command injection. Successful exploitation of this vulnerability may allow the attacker to execute system commands.	6.3	More Details
CVE-2024-5405	A vulnerability had been discovered in WinNMP 19.02 consisting of an XSS attack via /tools/redis.php page in the k, hash, key and p parameters. This vulnerability could allow a remote user to submit a specially crafted JavaScript payload for an authenticated user to retrieve their session details.	6.3	More Details
CVE-2024-5390	A vulnerability, which was classified as critical, was found in itsourcecode Online Student Enrollment System 1.0. Affected is an unknown function of the file listofstudent.php. The manipulation of the argument lname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266304.	6.3	More Details
CVE-2024-5378	A vulnerability was found in SourceCodester School Intramurals Student Attendance Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /manage_sy.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-266290 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-36112	Nautobot is a Network Source of Truth and Network Automation Platform. A user with permissions to view Dynamic Group records (`extras.view_dynamicgroup` permission) can use the Dynamic Group detail UI view (`/extras/dynamic-groups/<uuid>/`) and/or the members REST API view (`/api/extras/dynamic-groups/<uuid>/members/`) to list the objects that are members of a given Dynamic Group. In versions of Nautobot between 1.3.0 (where the Dynamic Groups feature was added) and 1.6.22 inclusive, and 2.0.0 through 2.2.4 inclusive, Nautobot fails to restrict these listings based on the member object permissions - for example a Dynamic Group of Device objects will list all Devices that it contains, regardless of the user's `dcim.view_device` permissions or lack thereof. This issue has been fixed in Nautobot versions 1.6.23 and 2.2.5. Users are advised to upgrade. This vulnerability can be partially mitigated by removing `extras.view_dynamicgroup` permission from users however a full fix will require upgrading.	6.3	More Details
CVE-2024-35555	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/share_switch.php?mudi=switch&dataType=newsWeb&fieldName=state&fieldName2=state&tabName=infoWeb&dataID=40.	6.3	More Details
CVE-2024-5234	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /view/teacher_salary_history1.php. The manipulation of the argument index leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-265985 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5238	A vulnerability, which was classified as critical, was found in Campcodes Complete Web-Based School Management System 1.0. This affects an unknown part of the file /view/timetable_insert_form.php. The manipulation of the argument grade leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-265989 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5231	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view/teacher_salary_details.php. The manipulation of the argument index leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-265982 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5232	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as critical. This affects an unknown part of the file /view/teacher_salary_details2.php. The manipulation of the argument index leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-265983.	6.3	More Details
CVE-2024-5233	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /view/teacher_salary_details3.php. The manipulation of the argument index leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-265984.	6.3	More Details
CVE-2024-5239	A vulnerability has been found in Campcodes Complete Web-Based School Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /view/timetable_update_form.php. The manipulation of the argument grade leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-265990 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5240	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /view/unread_msg.php. The manipulation of the argument my_index leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-265991.	6.3	More Details
CVE-2024-5235	A vulnerability classified as critical has been found in Campcodes Complete Web-Based School Management System 1.0. Affected is an unknown function of the file /view/teacher_salary_invoice.php. The manipulation of the argument teacher_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-265986 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5236	A vulnerability classified as critical was found in Campcodes Complete Web-Based School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view/teacher_salary_invoice1.php. The manipulation of the argument date leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-265987.	6.3	More Details
CVE-2024-34933	A SQL injection vulnerability in /model/update_grade.php in Campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the admission_fee parameter.	6.3	More Details
CVE-2024-35082	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in SysOperLogMapper.xml.	6.3	More Details
CVE-2024-5237	A vulnerability, which was classified as critical, has been found in Campcodes Complete Web-Based School Management System 1.0. Affected by this issue is some unknown functionality of the file /view/timetable_grade_wise.php. The manipulation of the argument grade leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-265988.	6.3	More Details
CVE-2021-47503	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Do not call scsi_remove_host() in pm8001_alloc() Calling scsi_remove_host() before scsi_add_host() results in a crash: BUG: kernel NULL pointer dereference, address: 0000000000000108 RIP: 0010:device_del+0x63/0x440 Call Trace: device_unregister+0x17/0x60 scsi_remove_host+0xee/0x2a0 pm8001_pci_probe+0x6ef/0x1b90 [pm80xx] local_pci_probe+0x3f/0x90 We cannot call scsi_remove_host() in pm8001_alloc() because scsi_add_host() has not been called yet at that point in time. Function call tree: pm8001_pci_probe() | `- pm8001_pci_alloc() | | `- pm8001_alloc() | | `- scsi_remove_host() | `- scsi_add_host()	6.2	More Details
CVE-2024-29421	xmedcon 0.23.0 and fixed in v.0.24.0 is vulnerable to Buffer Overflow via libs/dicom/basic.c which allows an attacker to execute arbitrary code.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47535	In the Linux kernel, the following vulnerability has been resolved: drm/msm/a6xx: Allocate enough space for GMU registers In commit 142639a52a01 ("drm/msm/a6xx: fix crashstate capture for A650") we changed a6xx_get_gmu_registers() to read 3 sets of registers. Unfortunately, we didn't change the memory allocation for the array. That leads to a KASAN warning (this was on the chromeos-5.4 kernel, which has the problematic commit backported to it): BUG: KASAN: slab-out-of-bounds in _a6xx_get_gmu_registers+0x144/0x430 Write of size 8 at addr ffffff80c89432b0 by task A618-worker/209 CPU: 5 PID: 209 Comm: A618-worker Tainted: G W 5.4.156-lockdep #22 Hardware name: Google Lazor Limozeen without Touchscreen (rev5 - rev8) (DT) Call trace: dump_backtrace+0x0/0x248 show_stack+0x20/0x2c dump_stack+0x128/0x1ec print_address_description+0x88/0x4a0 __kasan_report+0xfc/0x120 kasan_report+0x10/0x18 __asan_report_store8_noabort+0x1c/0x24 _a6xx_get_gmu_registers+0x144/0x430 a6xx_gpu_state_get+0x330/0x25d4 msm_gpu_crashstate_capture+0xa0/0x84c recover_worker+0x328/0x838 kthread_worker_fn+0x32c/0x574 kthread+0x2dc/0x39c ret_from_fork+0x10/0x18 Allocated by task 209: __kasan_kmalloc+0xfc/0x1c4 kasan_kmalloc+0xc/0x14 kmem_cache_alloc_trace+0x1f0/0x2a0 a6xx_gpu_state_get+0x164/0x25d4 msm_gpu_crashstate_capture+0xa0/0x84c recover_worker+0x328/0x838 kthread_worker_fn+0x32c/0x574 kthread+0x2dc/0x39c ret_from_fork+0x10/0x18	6.2	More Details
CVE-2024-4534	The KKProgressbar2 Free WordPress plugin through 1.1.4.2 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	6.1	More Details
CVE-2024-35595	An arbitrary file upload vulnerability in the File Preview function of Xintongda OA v2023.12.30.1 allows attackers to execute arbitrary code via uploading a crafted PDF file.	6.1	More Details
CVE-2024-36384	Pointsharp Cryptshare Server before 7.0.0 has an XSS issue that is related to notification messages.	6.1	More Details
CVE-2024-31395	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.12, Ver.3.0.x series versions prior to Ver.3.0.32, Ver.2.11.x series versions prior to Ver.2.11.61, Ver.2.10.x series versions prior to Ver.2.10.53, and Ver.2.9 and earlier versions. If this vulnerability is exploited, a user with an editor or higher privilege who can log in to the product may execute an arbitrary script on the web browser of the user who accessed the schedule management page.	6.1	More Details
CVE-2024-3519	The Media Library Assistant plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the lang parameter in all versions up to, and including, 3.15 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-2024-35291	Cross-site scripting vulnerability exists in Splunk Config Explorer versions prior to 1.7.16. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who is using the product.	6.1	More Details
CVE-2024-35581	A cross-site scripting (XSS) vulnerability in Sourcecodester Laboratory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Borrower Name input field.	6.1	More Details
CVE-2024-35582	A cross-site scripting (XSS) vulnerability in Sourcecodester Laboratory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Department input field.	6.1	More Details
CVE-2024-35583	A cross-site scripting (XSS) vulnerability in Sourcecodester Laboratory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Remarks input field.	6.1	More Details
CVE-2024-4563	The Progress MOVEit Automation configuration export function prior to 2024.0.0 uses a cryptographic method with insufficient bit length.	6.1	More Details
CVE-2024-1762	The NextScripts: Social Networks Auto-Poster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTTP_USER_AGENT header in all versions up to, and including, 4.4.3 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. This requires the victim to select view "All Cron Events" in order for the injection to fire.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35627	tileserver-gl up to v4.4.10 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /data/v3/?key.	6.1	More Details
CVE-2024-34923	In Avocent DSR2030 Appliance firmware 03.04.00.07 before 03.07.01.23, and SVIP1020 Appliance firmware 01.06.00.03 before 01.07.00.00, there is reflected cross-site scripting (XSS).	6.1	More Details
CVE-2024-2119	The LuckyWP Table of Contents plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the attrs parameter in all versions up to, and including, 2.1.4 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-2024-3917	The Pet Manager WordPress plugin through 1.4 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-2024-35182	Meshery is an open source, cloud native manager that enables the design and management of Kubernetes-based infrastructure and applications. A SQL injection vulnerability in Meshery prior to version 0.7.22 may lead to arbitrary file write by using a SQL injection stacked queries payload, and the ATTACH DATABASE command. Additionally, attackers may be able to access and modify any data stored in the database, like performance profiles (which may contain session cookies), Meshery application data, or any Kubernetes configuration added to the system. The Meshery project exposes the function `GetAllEvents` at the API URL `/api/v2/events`. The sort query parameter read in `events_streamer.go` is directly used to build a SQL query in `events_persister.go`. Version 0.7.22 fixes this issue by using the `SanitizeOrderInput` function.	5.9	More Details
CVE-2024-35181	Meshery is an open source, cloud native manager that enables the design and management of Kubernetes-based infrastructure and applications. A SQL injection vulnerability in Meshery prior to version 0.7.22 may lead to arbitrary file write by using a SQL injection stacked queries payload, and the ATTACH DATABASE command. Additionally, attackers may be able to access and modify any data stored in the database, like performance profiles (which may contain session cookies), Meshery application data, or any Kubernetes configuration added to the system. The Meshery project exposes the function `GetMeshSyncResourcesKinds` at the API URL `/api/system/meshsync/resources/kinds`. The order query parameter is directly used to build a SQL query in `meshync_handler.go`. Version 0.7.22 fixes this issue.	5.9	More Details
CVE-2024-5264	Network Transfer with AES KHT in Thales Luna EFT 2.1 and above allows a user with administrative console access to access backups taken via offline analysis	5.9	More Details
CVE-2024-35401	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a command injection vulnerability via the FileName parameter in the UploadFirmwareFile function.	5.9	More Details
CVE-2024-32045	Mattermost versions 9.5.x <= 9.5.3, 9.6.x <= 9.6.1, 8.1.x <= 8.1.12 fail to enforce proper access controls for channel and team membership when linking a playbook run to a channel which allows members to link their runs to private channels they were not members of.	5.9	More Details
CVE-2024-35222	Tauri is a framework for building binaries for all major desktop platforms. Remote origin iFrames in Tauri applications can access the Tauri IPC endpoints without being explicitly allowed in the `dangerousRemoteDomainIpcAccess` in v1 and in the `capabilities` in v2. Valid commands with potentially unwanted consequences ("delete project", "transfer credits", etc.) could be invoked by an attacker that controls the content of an iframe running inside a Tauri app. This vulnerability has been patched in versions 1.6.7 and 2.0.0-beta.19.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20293	A vulnerability in the activation of an access control list (ACL) on Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the protection that is offered by a configured ACL on an affected device. This vulnerability is due to a logic error that occurs when an ACL changes from inactive to active in the running configuration of an affected device. An attacker could exploit this vulnerability by sending traffic through the affected device that should be denied by the configured ACL. The reverse condition is also true—traffic that should be permitted could be denied by the configured ACL. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device, allowing the attacker to access trusted networks that the device might be protecting. Note: This vulnerability applies to both IPv4 and IPv6 traffic as well as dual-stack ACL configurations in which both IPv4 and IPv6 ACLs are configured on an interface.	5.8	More Details
CVE-2024-20361	A vulnerability in the Object Groups for Access Control Lists (ACLs) feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass configured access controls on managed devices that are running Cisco Firepower Threat Defense (FTD) Software. This vulnerability is due to the incorrect deployment of the Object Groups for ACLs feature from Cisco FMC Software to managed FTD devices in high-availability setups. After an affected device is rebooted following Object Groups for ACLs deployment, an attacker can exploit this vulnerability by sending traffic through the affected device. A successful exploit could allow the attacker to bypass configured access controls and successfully send traffic to devices that are expected to be protected by the affected device.	5.8	More Details
CVE-2024-20261	A vulnerability in the file policy feature that is used to inspect encrypted archive files of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured file policy to block an encrypted archive file. This vulnerability exists because of a logic error when a specific class of encrypted archive files is inspected. An attacker could exploit this vulnerability by sending a crafted, encrypted archive file through the affected device. A successful exploit could allow the attacker to send an encrypted archive file, which could contain malware and should have been blocked and dropped at the Cisco FTD device.	5.8	More Details
CVE-2024-20363	Multiple Cisco products are affected by a vulnerability in the Snort Intrusion Prevention System (IPS) rule engine that could allow an unauthenticated, remote attacker to bypass the configured rules on an affected system. This vulnerability is due to incorrect HTTP packet handling. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured IPS rules and allow uninspected traffic onto the network.	5.8	More Details
CVE-2024-36255	Mattermost versions 9.5.x <= 9.5.3, 9.6.x <= 9.6.1 and 8.1.x <= 8.1.12 fail to perform proper input validation on post actions which allows an attacker to run a playbook checklist task command as another user via creating and sharing a deceptive post action that unexpectedly runs a slash command in some arbitrary channel.	5.7	More Details
CVE-2024-2199	A denial of service vulnerability was found in 389-ds-base ldap server. This issue may allow an authenticated user to cause a server crash while modifying `userPassword` using malformed input.	5.7	More Details
CVE-2021-47509	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Limit the period size to 16MB Set the practical limit to the period size (the fragment shift in OSS) instead of a full 31bit; a too large value could lead to the exhaust of memory as we allocate temporary buffers of the period size, too. As of this patch, we set to 16MB limit, which should cover all use cases.	5.5	More Details
CVE-2024-36055	Hw64.sys in Marvin Test HW.exe before 5.0.5.0 allows unprivileged user-mode processes to arbitrarily map physical memory with read/write access via the MmMapIoSpace API (IOCTL 0x9c40a4f8, 0x9c40a4e8, 0x9c40a4c0, 0x9c40a4c4, 0x9c40a4ec, and seven others), leading to a denial of service (BSOD).	5.5	More Details
CVE-2021-47529	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: Fix memory leaks in error handling path Should an error occur (invalid TLV len or memory allocation failure), the memory already allocated in 'reduce_power_data' should be freed before returning, otherwise it is leaking.	5.5	More Details
CVE-2021-47528	In the Linux kernel, the following vulnerability has been resolved: usb: cdnsp: Fix a NULL pointer dereference in cdnsp_endpoint_init() In cdnsp_endpoint_init(), cdnsp_ring_alloc() is assigned to pep->ring and there is a dereference of it in cdnsp_endpoint_init(), which could lead to a NULL pointer dereference on failure of cdnsp_ring_alloc(). Fix this bug by adding a check of pep->ring. 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_USB_CDNSP_GADGET=y show no new warnings, and our static analyzer no longer warns about this code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47511	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix negative period/buffer sizes The period size calculation in OSS layer may receive a negative value as an error, but the code there assumes only the positive values and handle them with size_t. Due to that, a too big value may be passed to the lower layers. This patch changes the code to handle with ssize_t and adds the proper error checks appropriately.	5.5	More Details
CVE-2021-47471	In the Linux kernel, the following vulnerability has been resolved: drm: mxsfb: Fix NULL pointer dereference crash on unload The mxsfb->crtc.funcs may already be NULL when unloading the driver, in which case calling mxsfb_irq_disable() via drm_irq_uninstall() from mxsfb_unload() leads to NULL pointer dereference. Since all we care about is masking the IRQ and mxsfb->base is still valid, just use that to clear and mask the IRQ.	5.5	More Details
CVE-2021-47526	In the Linux kernel, the following vulnerability has been resolved: serial: liteuart: Fix NULL pointer dereference in ->remove() drvdata has to be set in _probe() - otherwise platform_get_drvdata() causes null pointer dereference BUG in _remove().	5.5	More Details
CVE-2021-47513	In the Linux kernel, the following vulnerability has been resolved: net: dsa: felix: Fix memory leak in felix_setup_mmio_filtering Avoid a memory leak if there is not a CPU port defined. Addresses-Coverity-ID: 1492897 ("Resource leak") Addresses-Coverity-ID: 1492899 ("Resource leak")	5.5	More Details
CVE-2024-2953	The LuckyWP Table of Contents plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 2.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Contributor permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2021-47516	In the Linux kernel, the following vulnerability has been resolved: nfp: Fix memory leak in nfp_cpp_area_cache_add() In line 800 (#1), nfp_cpp_area_alloc() allocates and initializes a CPP area structure. But in line 807 (#2), when the cache is allocated failed, this CPP area structure is not freed, which will result in memory leak. We can fix it by freeing the CPP area when the cache is allocated failed (#2). 792 int nfp_cpp_area_cache_add(struct nfp_cpp *cpp, size_t size) 793 { 794 struct nfp_cpp_area_cache *cache; 795 struct nfp_cpp_area *area; 800 area = nfp_cpp_area_alloc(cpp, NFP_CPP_ID(7, NFP_CPP_ACTION_RW, 0), 801 0, size); // #1: allocates and initializes 802 if (!area) 803 return -ENOMEM; 805 cache = kzalloc(sizeof(*cache), GFP_KERNEL); 806 if (!cache) 807 return -ENOMEM; // #2: missing free 817 return 0; 818 }	5.5	More Details
CVE-2021-47518	In the Linux kernel, the following vulnerability has been resolved: nfc: fix potential NULL pointer deref in nfc_genl_dump_ses_done The done() netlink callback nfc_genl_dump_ses_done() should check if received argument is non-NULL, because its allocation could fail earlier in dumpit() (nfc_genl_dump_ses()).	5.5	More Details
CVE-2021-47519	In the Linux kernel, the following vulnerability has been resolved: can: m_can: m_can_read_fifo: fix memory leak in error branch In m_can_read_fifo(), if the second call to m_can_fifo_read() fails, the function jump to the out_fail label and returns without calling m_can_receive_skb(). This means that the skb previously allocated by alloc_can_skb() is not freed. In other terms, this is a memory leak. This patch adds a goto label to destroy the skb if an error occurs. Issue was found with GCC -fanalyzer, please follow the link below for details.	5.5	More Details
CVE-2021-47484	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: Fix possible null pointer dereference. This patch fixes possible null pointer dereference in files "rvu_debugfs.c" and "rvu_nix.c"	5.5	More Details
CVE-2021-47537	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: Fix a memleak bug in rvu_mbox_init() In rvu_mbox_init(), mbox_regions is not freed or passed out under the switch-default region, which could lead to a memory leak. Fix this bug by changing 'return err' to 'goto free_regions'. 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_OCTEONTX2_AF=y show no new warnings, and our static analyzer no longer warns about this code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47572	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: fix null pointer dereference when IPv6 is not enabled When we try to add an IPv6 nexthop and IPv6 is not enabled (!CONFIG_IPV6) we'll hit a NULL pointer dereference[1] in the error path of nh_create_ipv6() due to calling ipv6_stub->fib6_nh_release. The bug has been present since the beginning of IPv6 nexthop gateway support. Commit 1aefd3de7bc6 ("ipv6: Add fib6_nh_init and release to stubs") tells us that only fib6_nh_init has a dummy stub because fib6_nh_release should not be called if fib6_nh_init returns an error, but the commit below added a call to ipv6_stub->fib6_nh_release in its error path. To fix it return the dummy stub's -EAFNOSUPPORT error directly without calling ipv6_stub->fib6_nh_release in nh_create_ipv6()'s error path. [1] Output is a bit truncated, but it clearly shows the error. BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor instruction fetch in kernel modede #PF: error_code(0x0010) - not-present pagege PGD 0 P4D 0 Oops: 0010 [#1] PREEMPT SMP NOPTI CPU: 4 PID: 638 Comm: ip Kdump: loaded Not tainted 5.16.0-rc1+ #446 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-4.fc34 04/01/2014 RIP: 0010:0x0 Code: Unable to access opcode bytes at RIP 0xffffffffffffffd6. RSP: 0018:ffff888109f5b8f0 EFLAGS: 00010286^Ac RAX: 0000000000000000 RBX: ffff888109f5ba28 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff8881008a2860 RBP: ffff888109f5b9d8 R08: 0000000000000000 R09: 0000000000000000 R10: ffff888109f5b978 R11: ffff888109f5b948 R12: 00000000ffffff9f R13: ffff8881008a2a80 R14: ffff8881008a2860 R15: ffff8881008a2840 FS: 00007f98de70f100(0000) GS:ffff88822bf00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffffffffd6 CR3: 0000000100efc000 CR4: 00000000000006e0 Call Trace: <TASK> nh_create_ipv6+0xed/0x10c rtm_new_nexthop+0x6d7/0x13f3 ? check_preemption_disabled+0x3d/0xf2 ? lock_is_held_type+0xbe/0xfd rtnetlink_rcv_msg+0x23f/0x26a ? check_preemption_disabled+0x3d/0xf2 ? rtnl_calcit.isra.0+0x147/0x147 netlink_rcv_skb+0x61/0xb2 netlink_unicast+0x100/0x187 netlink_sendmsg+0x37f/0x3a0 ? netlink_unicast+0x187/0x187 sock_sendmsg_nosec+0x67/0x9b ____sys_sendmsg+0x19d/0x1f9 ? copy_msghdr_from_user+0x4c/0x5e ? rcu_read_lock_any_held+0x2a/0x78 ___sys_sendmsg+0x6c/0x8c ? asm_sysvec_apic_timer_interrupt+0x12/0x20 ? lockdep_hardirqs_on+0xd9/0x102 ? sockfd_lookup_light+0x69/0x99 __sys_sendmsg+0x50/0x6e do_syscall_64+0xcb/0xf2 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f98dea28914 Code: 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b5 0f 1f 80 00 00 00 00 48 8d 05 e9 5d 0c 00 8b 00 85 c0 75 13 b8 2e 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 41 54 41 89 d4 55 48 89 f5 53 RSP: 002b:00007fff859f5e68 EFLAGS: 00000246 ORIG_RAX: 000000000000002e2e RAX: ffffffffffffffda RBX: 00000000619cb810 RCX: 00007f98dea28914 RDX: 0000000000000000 RSI: 00007fff859f5ed0 RDI: 0000000000000003 RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000008 R10: fffffffffffffce6 R11: 0000000000000246 R12: 0000000000000001 R13: 000055c0097ae520 R14: 000055c0097957fd R15: 00007fff859f63a0 </TASK> Modules linked in: bridge stp llc bonding virtio_net	5.5	More Details
CVE-2021-47570	In the Linux kernel, the following vulnerability has been resolved: staging: r8188eu: fix a memory leak in rtw_wx_read32() Free "ptmp" before returning -EINVAL.	5.5	More Details
CVE-2021-47498	In the Linux kernel, the following vulnerability has been resolved: dm rq: don't queue request to blk-mq during DM suspend DM uses blk-mq's quiesce/unquiesce to stop/start device mapper queue. But blk-mq's unquiesce may come from outside events, such as elevator switch, updating nr_requests or others, and request may come during suspend, so simply ask for blk-mq to requeue it. Fixes one kernel panic issue when running updating nr_requests and dm-mpath suspend/resume stress test.	5.5	More Details
CVE-2024-35557	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/vpsApi_deal.php?mudi=rev&nohrefStr=close.	5.5	More Details
CVE-2021-47522	In the Linux kernel, the following vulnerability has been resolved: HID: bigbenff: prevent null pointer dereference When emulating the device through uhid, there is a chance we don't have output reports and so report_field is null.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47563	In the Linux kernel, the following vulnerability has been resolved: ice: avoid bpf_prog refcount underflow Ice driver has the routines for managing XDP resources that are shared between ndo_bpf op and VSI rebuild flow. The latter takes place for example when user changes queue count on an interface via ethtool's set_channels(). There is an issue around the bpf_prog refcounting when VSI is being rebuilt - since ice_prepare_xdp_rings() is called with vsi->xdp_prog as an argument that is used later on by ice_vsi_assign_bpf_prog(), same bpf_prog pointers are swapped with each other. Then it is also interpreted as an 'old_prog' which in turn causes us to call bpf_prog_put on it that will decrement its refcount. Below splat can be interpreted in a way that due to zero refcount of a bpf_prog it is wiped out from the system while kernel still tries to refer to it: [481.069429] BUG: unable to handle page fault for address: ffffc9000640f038 [481.077390] #PF: supervisor read access in kernel mode [481.083335] #PF: error_code(0x0000) - not-present page [481.089276] PGD 100000067 P4D 100000067 PUD 1001cb067 PMD 106d2b067 PTE 0 [481.097141] Oops: 0000 [#1] PREEMPT SMP PTI [481.101980] CPU: 12 PID: 3339 Comm: sudo Tainted: G OE 5.15.0-rc5+ #1 [481.110840] Hardware name: Intel Corp. GRANTLEY/GRANTLEY, BIOS GRRFCRB1.86B.0276.D07.1605190235 05/19/2016 [481.122021] RIP: 0010:dev_xdp_prog_id+0x25/0x40 [481.127265] Code: 80 00 00 00 00 0f 1f 44 00 00 89 f6 48 c1 e6 04 48 01 fe 48 8b 86 98 08 00 00 48 85 c0 74 13 48 8b 50 18 31 c0 48 85 d2 74 07 <48> 8b 42 38 8b 40 20 c3 48 8b 96 90 08 00 00 eb e8 66 2e 0f 1f 84 [481.148991] RSP: 0018:ffffc90007b63868 EFLAGS: 00010286 [481.155034] RAX: 0000000000000000 RBX: ffff889080824000 RCX: 0000000000000000 [481.163278] RDX: ffffc9000640f000 RSI: ffff889080824010 RDI: ffff889080824000 [481.171527] RBP: ffff888107af7d00 R08: 0000000000000000 R09: ffff88810db5f6e0 [481.179776] R10: 0000000000000000 R11: ffff8890885b9988 R12: ffff88810db5f4bc [481.188026] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [481.196276] FS: 00007f5466d5bec0(0000) GS:ffff88903fb00000(0000) knlGS:0000000000000000 [481.205633] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [481.212279] CR2: ffffc9000640f038 CR3: 000000014429c006 CR4: 00000000003706e0 [481.220530] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [481.228771] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [481.237029] Call Trace: [481.239856] rtnl_fill_ifinfo+0x768/0x12e0 [481.244602] rtnl_dump_ifinfo+0x525/0x650 [481.249246] ? __alloc_skb+0xa5/0x280 [481.253484] netlink_dump+0x168/0x3c0 [481.257725] netlink_recvmsg+0x21e/0x3e0 [481.262263] ____sys_recvmsg+0x87/0x170 [481.266707] ? __might_fault+0x20/0x30 [481.271046] ? _copy_from_user+0x66/0xa0 [481.275591] ? iovec_from_user+0xf6/0x1c0 [481.280226] ___sys_recvmsg+0x82/0x100 [481.284566] ? sock_sendmsg+0x5e/0x60 [481.288791] ? __sys_sendto+0xee/0x150 [481.293129] __sys_recvmsg+0x56/0xa0 [481.297267] do_syscall_64+0x3b/0xc0 [481.301395] entry_SYSCALL_64_after_hwframe+0x44/0xae [481.307238] RIP: 0033:0x7f5466f39617 [481.311373] Code: 0c 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb bd 0f 1f 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75 10 b8 2f 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 51 c3 48 83 ec 28 89 54 24 1c 48 89 74 24 10 [481.342944] RSP: 002b:00007ffedc7f4308 EFLAGS: 00000246 ORIG_RAX: 000000000000002f [481.361783] RAX: ffffffffffffffda RBX: 00007ffedc7f5460 RCX: 00007f5466f39617 [481.380278] RDX: 0000000000000000 RSI: 00007ffedc7f5360 RDI: 0000000000000003 [481.398500] RBP: 00007ffedc7f53f0 R08: 0000000000000000 R09: 000055d556f04d50 [481.416463] R10: 0000000000000077 R11: 0000000000000246 R12: 00007ffedc7f5360 [481.434131] R13: 00007ffedc7f5350 R14: 00007ffedc7f5344 R15: 0000000000000e98 [481.451520] Modules linked in: ice ---truncated---	5.5	More Details
CVE-2021-47559	In the Linux kernel, the following vulnerability has been resolved: net/smc: Fix NULL pointer dereferencing in smc_vlan_by_tcpsk() Coverity reports a possible NULL dereferencing problem: in smc_vlan_by_tcpsk(): 6. returned_null: netdev_lower_get_next returns NULL (checked 29 out of 30 times). 7. var_assigned: Assigning: ndev = NULL return value from netdev_lower_get_next. 1623 ndev = (struct net_device *)netdev_lower_get_next(ndev, &lower); CID 1468509 (#1 of 1): Dereference null return value (NULL_RETURNS) 8. dereference: Dereferencing a pointer that might be NULL ndev when calling is_vlan_dev. 1624 if (is_vlan_dev(ndev)) { Remove the manual implementation and use netdev_walk_all_lower_dev() to iterate over the lower devices. While on it remove an obsolete function parameter comment.	5.5	More Details
CVE-2021-47556	In the Linux kernel, the following vulnerability has been resolved: ethtool: ioctl: fix potential NULL deref in ethtool_set_coalesce() ethtool_set_coalesce() now uses both the .get_coalesce() and .set_coalesce() callbacks. But the check for their availability is buggy, so changing the coalesce settings on a device where the driver provides only _one_ of the callbacks results in a NULL pointer dereference instead of an -EOPNOTSUPP. Fix the condition so that the availability of both callbacks is ensured. This also matches the netlink code. Note that reproducing this requires some effort - it only affects the legacy ioctl path, and needs a specific combination of driver options: - have .get_coalesce() and .coalesce_supported but no .set_coalesce(), or - have .set_coalesce() but no .get_coalesce(). Here eg. ethtool doesn't cause the crash as it first attempts to call ethtool_get_coalesce() and bails out on error.	5.5	More Details
CVE-2021-47443	In the Linux kernel, the following vulnerability has been resolved: NFC: digital: fix possible memory leak in digital_tg_listen_mdaa() 'params' is allocated in digital_tg_listen_mdaa(), but not free when digital_send_cmd() failed, which will cause memory leak. Fix it by freeing 'params' if digital_send_cmd() return failed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36037	Zoho ManageEngine ADAudit Plus versions 7260 and below allows unauthorized local agent machine users to view the session recordings.	5.5	More Details
CVE-2021-47550	In the Linux kernel, the following vulnerability has been resolved: drm/amd/amdgpu: fix potential memleak In function amdgpu_get_xgmi_hive, when kobject_init_and_add failed There is a potential memleak if not call kobject_put.	5.5	More Details
CVE-2021-47546	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix memory leak in fib6_rule_suppress The kernel leaks memory when a `fib` rule is present in IPv6 nftables firewall rules and a suppress_prefix rule is present in the IPv6 routing rules (used by certain tools such as wg-quick). In such scenarios, every incoming packet will leak an allocation in `ip6_dst_cache` slab cache. After some hours of `bpftrace`-ing and source code reading, I tracked down the issue to ca7a03c41753 ("ipv6: do not free rt if FIB_LOOKUP_NOREF is set on suppress rule"). The problem with that change is that the generic `args->flags` always have `FIB_LOOKUP_NOREF` set[1][2] but the IPv6-specific flag `RT6_LOOKUP_F_DST_NOREF` might not be, leading to `fib6_rule_suppress` not decreasing the refcount when needed. How to reproduce: - Add the following nftables rule to a prerouting chain: meta nfproto ipv6 fib saddr . mark . iif oif missing drop This can be done with: sudo nft create table inet test sudo nft create chain inet test test_chain '{ type filter hook prerouting priority filter + 10; policy accept; }' sudo nft add rule inet test test_chain meta nfproto ipv6 fib saddr . mark . iif oif missing drop - Run: sudo ip -6 rule add table main suppress_prefixlength 0 - Watch `sudo slabtop -o	grep ip6_dst_cache` to see memory usage increase with every incoming ipv6 packet. This patch exposes the protocol-specific flags to the protocol specific `suppress` function, and check the protocol-specific `flags` argument for RT6_LOOKUP_F_DST_NOREF instead of the generic FIB_LOOKUP_NOREF when decreasing the refcount, like this. [1]: https://github.com/torvalds/linux/blob/ca7a03c4175366a92cee0ccc4fec0038c3266e26/net/ipv6/fib6_rules.c#L71 [2]: https://github.com/torvalds/linux/blob/ca7a03c4175366a92cee0ccc4fec0038c3266e26/net/ipv6/fib6_rules.c#L99	5.5	More Details
CVE-2021-47439	In the Linux kernel, the following vulnerability has been resolved: net: dsa: microchip: Added the condition for scheduling ksz_mib_read_work When the ksz module is installed and removed using rmmod, kernel crashes with null pointer dereferrence error. During rmmod, ksz_switch_remove function tries to cancel the mib_read_workqueue using cancel_delayed_work_sync routine and unregister switch from dsa. During dsa_unregister_switch it calls ksz_mac_link_down, which in turn reschedules the workqueue since mib_interval is non-zero. Due to which queue executed after mib_interval and it tries to access dp->slave. But the slave is unregistered in the ksz_switch_remove function. Hence kernel crashes. To avoid this crash, before canceling the workqueue, resetted the mib_interval to 0. v1 -> v2: -Removed the if condition in ksz_mib_read_work	5.5	More Details
CVE-2021-47542	In the Linux kernel, the following vulnerability has been resolved: net: qlogic: qlcnic: Fix a NULL pointer dereference in qlcnic_83xx_add_rings() In qlcnic_83xx_add_rings(), the indirect function of ahw->hw_ops->alloc_mbx_args will be called to allocate memory for cmd.req.arg, and there is a dereference of it in qlcnic_83xx_add_rings(), which could lead to a NULL pointer dereference on failure of the indirect function like qlcnic_83xx_alloc_mbx_args(). Fix this bug by adding a check of alloc_mbx_args(), this patch imitates the logic of mbx_cmd()'s failure handling. 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_QLCNIC=m show no new warnings, and our static analyzer no longer warns about this code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47540	In the Linux kernel, the following vulnerability has been resolved: mt76: mt7915: fix NULL pointer dereference in mt7915_get_phy_mode Fix the following NULL pointer dereference in mt7915_get_phy_mode routine adding an ibss interface to the mt7915 driver. [101.137097] wlan0: Trigger new scan to find an IBSS to join [102.827039] wlan0: Creating new IBSS network, BSSID 26:a4:50:1a:6e:69 [103.064756] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [103.073670] Mem abort info: [103.076520] ESR = 0x96000005 [103.079614] EC = 0x25: DABT (current EL), IL = 32 bits [103.084934] SET = 0, FnV = 0 [103.088042] EA = 0, S1PTW = 0 [103.091215] Data abort info: [103.094104] ISV = 0, ISS = 0x00000005 [103.098041] CM = 0, WnR = 0 [103.101044] user pgtable: 4k pages, 39-bit VAs, pgdp=00000000460b1000 [103.107565] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000, pud=0000000000000000 [103.116590] Internal error: Oops: 96000005 [#1] SMP [103.189066] CPU: 1 PID: 333 Comm: kworker/u4:3 Not tainted 5.10.75 #0 [103.195498] Hardware name: MediaTek MT7622 RFB1 board (DT) [103.201124] Workqueue: phy0 ieee80211_iface_work [mac80211] [103.206695] pstate: 20000005 (nzCv daif -PAN -UAO -TCO BTYPE=--) [103.212705] pc : mt7915_get_phy_mode+0x68/0x120 [mt7915e] [103.218103] lr : mt7915_mcu_add_bss_info+0x11c/0x760 [mt7915e] [103.223927] sp : ffffffc011cdb9e0 [103.227235] x29: ffffffc011cdb9e0 x28: ffffff8006563098 [103.232545] x27: ffffff8005f4da22 x26: ffffff800685ac40 [103.237855] x25: 0000000000000001 x24: 000000000000011f [103.243165] x23: ffffff8005f4e260 x22: ffffff8006567918 [103.248475] x21: ffffff8005f4df80 x20: ffffff800685ac58 [103.253785] x19: ffffff8006744400 x18: 0000000000000000 [103.259094] x17: 0000000000000000 x16: 0000000000000001 [103.264403] x15: 000899c3a2d9d2e4 x14: 000899bdc3c3a1c8 [103.269713] x13: 0000000000000000 x12: 0000000000000000 [103.275024] x11: ffffffc010e30c20 x10: 0000000000000000 [103.280333] x9 : 0000000000000050 x8 : ffffff8006567d88 [103.285642] x7 : ffffff8006563b5c x6 : ffffff8006563b44 [103.290952] x5 : 0000000000000002 x4 : 0000000000000001 [103.296262] x3 : 0000000000000001 x2 : 0000000000000001 [103.301572] x1 : 0000000000000000 x0 : 0000000000000011 [103.306882] Call trace: [103.309328] mt7915_get_phy_mode+0x68/0x120 [mt7915e] [103.314378] mt7915_bss_info_changed+0x198/0x200 [mt7915e] [103.319941] ieee80211_bss_info_change_notify+0x128/0x290 [mac80211] [103.326360] __ieee80211_sta_join_ibss+0x308/0x6c4 [mac80211] [103.332171] ieee80211_sta_create_ibss+0x8c/0x10c [mac80211] [103.337895] ieee80211_ibss_work+0x3dc/0x614 [mac80211] [103.343185] ieee80211_iface_work+0x388/0x3f0 [mac80211] [103.348495] process_one_work+0x288/0x690 [103.352499] worker_thread+0x70/0x464 [103.356157] kthread+0x144/0x150 [103.359380] ret_from_fork+0x10/0x18 [103.362952] Code: 394008c3 52800220 394000e4 7100007f (39400023)	5.5	More Details
CVE-2024-35593	An arbitrary file upload vulnerability in the File preview function of Raingad IM v4.1.4 allows attackers to execute arbitrary code via uploading a crafted PDF file.	5.5	More Details
CVE-2021-47478	In the Linux kernel, the following vulnerability has been resolved: isofs: Fix out of bound access for corrupted isofs image When isofs image is suitably corrupted isofs_read_inode() can read data beyond the end of buffer. Sanity-check the directory entry length before using it.	5.5	More Details
CVE-2024-29392	Silverpeas Core 6.3 is vulnerable to Cross Site Scripting (XSS) via ClipboardSessionController.	5.4	More Details
CVE-2024-4261	The Responsive Contact Form Builder & Lead Generation Plugin plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.9.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with subscriber-level access and above, to execute arbitrary shortcodes.	5.4	More Details
CVE-2024-25737	A Server-Side Request Forgery (SSRF) vulnerability in the /Cover/Show route (showAction in CoverController.php) in Open Library Foundation VuFind 2.4 through 9.1 before 9.1.1 allows remote attackers to access internal HTTP servers and perform Cross-Site Scripting (XSS) attacks by proxying arbitrary URLs via the proxy GET parameter.	5.4	More Details
CVE-2024-36056	Hw64.sys in Marvin Test HW.exe before 5.0.5.0 allows unprivileged user-mode processes to arbitrarily map physical memory via IOCTL 0x9c406490 (for IoAllocateMdl, MmBuildMdlForNonPagedPool, and MmMapLockedPages), leading to NT AUTHORITY\SYSTEM privilege escalation.	5.4	More Details
CVE-2024-35561	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/ca_deal.php?mudi=add&nohrefStr=close.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35085	J2EEFAST v2.7.0 was discovered to contain a SQL injection vulnerability via the findPage function in ProcessDefinitionMapper.xml.	5.4	More Details
CVE-2023-47710	IBM Security Guardium 11.4, 11.5, and 12.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 271525.	5.4	More Details
CVE-2024-35591	An arbitrary file upload vulnerability in O2OA v8.3.8 allows attackers to execute arbitrary code via uploading a crafted PDF file.	5.4	More Details
CVE-2024-35197	gitoxide is a pure Rust implementation of Git. On Windows, fetching refs that clash with legacy device names reads from the devices, and checking out paths that clash with such names writes arbitrary data to the devices. This allows a repository, when cloned, to cause indefinite blocking or the production of arbitrary message that appear to have come from the application, and potentially other harmful effects under limited circumstances. If Windows is not used, or untrusted repositories are not cloned or otherwise used, then there is no impact. A minor degradation in availability may also be possible, such as with a very large file named `CON`, though the user could interrupt the application.	5.4	More Details
CVE-2024-33803	A SQL injection vulnerability in /model/get_exam.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the id parameter.	5.4	More Details
CVE-2024-30419	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.12, Ver.3.0.x series versions prior to Ver.3.0.32, Ver.2.11.x series versions prior to Ver.2.11.61, Ver.2.10.x series versions prior to Ver.2.10.53, and Ver.2.9 and earlier versions. If this vulnerability is exploited, a user with a contributor or higher privilege who can log in to the product may execute an arbitrary script on the web browser of the user who accessed the website using the product.	5.4	More Details
CVE-2024-35548	A SQL injection vulnerability in Mybatis plus versions below 3.5.6 allows remote attackers to obtain database information via a Boolean blind injection. NOTE: the vendor's position is that this can only occur in a misconfigured application; the documentation discusses how to develop applications that avoid SQL injection.	5.4	More Details
CVE-2024-33807	A SQL injection vulnerability in /model/get_teacher_timetable.php in campcodes Complete Web-Based School Management System 1.0 allows an attacker to execute arbitrary SQL commands via the grade parameter.	5.4	More Details
CVE-2024-1446	The NextScripts: Social Networks Auto-Poster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.4.3. This is due to missing or incorrect nonce validation on the nxssnap-reposter page. This makes it possible for unauthenticated attackers to delete arbitrary posts or pages via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2024-4429	Cross-Site Request Forgery vulnerability has been discovered in OpenText™ iManager 3.2.6.0200. This could lead to sensitive information disclosure.	5.4	More Details
CVE-2024-35240	Umbraco Commerce is an open source dotnet ecommerce solution. In affected versions there exists a stored Cross-site scripting (XSS) issue which would enable attackers to inject malicious code into Print Functionality. This issue has been addressed in versions 12.1.4, and 10.0.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2023-7045	A CSRF vulnerability exists within GitLab CE/EE from versions 13.11 before 16.10.6, from 16.11 before 16.11.3, from 17.0 before 17.0.1. By leveraging this vulnerability, an attacker could exfiltrate anti-CSRF tokens via the Kubernetes Agent Server (KAS).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36107	MinIO is a High Performance Object Storage released under GNU Affero General Public License v3.0. `If-Modified-Since` and `If-Unmodified-Since` headers when used with anonymous requests by sending a random object name requests can be used to determine if an object exists or not on the server on a specific bucket and also gain access to some amount of information such as `Last-Modified (of the latest version)`, `Etag (of the latest version)`, `x-amz-version-id (of the latest version)`, `Expires (metadata value of the latest version)`, `Cache-Control (metadata value of the latest version)`. This conditional check was being honored before validating if the anonymous access is indeed allowed on the metadata of an object. This issue has been addressed in commit `e0fe7cc3917`. Users must upgrade to RELEASE.2024-05-27T19-17-46Z for the fix. There are no known workarounds for this issue.	5.3	More Details
CVE-2024-35229	ZKsync Era is a layer 2 rollup that uses zero-knowledge proofs to scale Ethereum. Prior to version 1.3.10, there is a very specific pattern `f(a(),b()); check_if_a_executed_last()` in Yul that exposes a bug in evaluation order of Yul function arguments. This vulnerability has been fixed in version 1.3.10. As a workaround, update and redeploy affected contracts.	5.3	More Details
CVE-2022-4969	A vulnerability, which was classified as critical, has been found in bwoodsend rockhopper up to 0.1.2. Affected by this issue is the function count_rows of the file rockhopper/src/ragged_array.c of the component Binary Parser. The manipulation of the argument raw leads to buffer overflow. Local access is required to approach this attack. Upgrading to version 0.2.0 is able to address this issue. The name of the patch is 1a15fad5e06ae693eb9b8908363d2c8ef455104e. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-266312.	5.3	More Details
CVE-2024-5193	A vulnerability was found in Ritlabs TinyWeb Server 1.94. It has been classified as problematic. Affected is an unknown function of the component Request Handler. The manipulation with the input %0D%0A leads to crlf injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-265830 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-35223	Dapr is a portable, event-driven, runtime for building distributed applications across cloud and edge. Dapr sends the app token of the invoker app instead of the app token of the invoked app. This causes of a leak of the application token of the invoker app to the invoked app when using Dapr as a gRPC proxy for remote service invocation. This vulnerability impacts Dapr users who use Dapr as a gRPC proxy for remote service invocation as well as the Dapr App API token functionality. An attacker could exploit this vulnerability to gain access to the app token of the invoker app, potentially compromising security and authentication mechanisms. This vulnerability was patched in version 1.13.3.	5.3	More Details
CVE-2021-47482	In the Linux kernel, the following vulnerability has been resolved: net: batman-adv: fix error handling Syzbot reported ODEBUG warning in batadv_nc_mesh_free(). The problem was in wrong error handling in batadv_mesh_init(). Before this patch batadv_mesh_init() was calling batadv_mesh_free() in case of any batadv_*_init() calls failure. This approach may work well, when there is some kind of indicator, which can tell which parts of batadv are initialized; but there isn't any. All written above lead to cleaning up uninitialized fields. Even if we hide ODEBUG warning by initializing bat_priv->nc.work, syzbot was able to hit GPF in batadv_nc_purge_paths(), because hash pointer in still NULL. [1] To fix these bugs we can unwind batadv_*_init() calls one by one. It is good approach for 2 reasons: 1) It fixes bugs on error handling path 2) It improves the performance, since we won't call unneeded batadv_*_free() functions. So, this patch makes all batadv_*_init() clean up all allocated memory before returning with an error to no call correspoing batadv_*_free() and open-codes batadv_mesh_free() with proper order to avoid touching uninitialized fields.	5.3	More Details
CVE-2024-36383	An issue was discovered in Logpoint SAML Authentication before 6.0.3. An attacker can place a crafted filename in the state field of a SAML SSO-URL response, and the file corresponding to this filename will ultimately be deleted. This can lead to a SAML Authentication login outage.	5.3	More Details
CVE-2021-47477	In the Linux kernel, the following vulnerability has been resolved: comedi: dt9812: fix DMA buffers on stack USB transfer buffers are typically mapped for DMA and must not be allocated on the stack or transfers will fail. Allocate proper transfer buffers in the various command helpers and return an error on short transfers instead of acting on random stack data. Note that this also fixes a stack info leak on systems where DMA is not used as 32 bytes are always sent to the device regardless of how short the command is.	5.3	More Details
CVE-2024-28188	Jupyter Scheduler is collection of extensions for programming jobs to run now or run on a schedule. The list of conda environments of `jupyter-scheduler` users maybe be exposed, potentially revealing information about projects that a specific user may be working on. This vulnerability has been patched in version(s) 1.1.6, 1.2.1, 1.8.2 and 2.5.2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1855	The WPCafe – Restaurant Menu, Online Ordering for WooCommerce, Pickup / Delivery and Table Reservation plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.2.23 via the wpc_check_for_submission function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application.	5.3	More Details
CVE-2023-43846	Incorrect access control in logs management function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote attackers to get the device logs via HTTP GET request. The logs contain such information as user names and IP addresses used in the infrastructure. This information may help the attackers to conduct further attacks in the infrastructure.	5.3	More Details
CVE-2023-6325	The RomethemeForm For Elementor plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the export_entries, rtformnewform, and rtformupdate functions in all versions up to, and including, 1.1.5. This makes it possible for unauthenticated attackers to export arbitrary form submissions, create new forms, or update any post title or certain metadata.	5.3	More Details
CVE-2023-43847	Incorrect access control in the outlet control function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote authenticated users to control all the outlets as if they were the administrator via HTTP POST requests.	5.3	More Details
CVE-2024-5230	A vulnerability has been found in EnvaySoft FleetCart up to 4.1.1 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument razorpayKeyId leads to information disclosure. The attack can be launched remotely. It is recommended to upgrade the affected component. The identifier VDB-265981 was assigned to this vulnerability.	5.3	More Details
CVE-2024-3933	In Eclipse OpenJ9 release versions prior to 0.44.0 and after 0.13.0, when running with JVM option -Xgc:concurrentScavenge, the sequence generated for System.arrayCopy on the IBM Z platform with hardware and software support for guarded storage [1], could allow access to a buffer with an incorrect length value when executing an arraycopy sequence while the Concurrent Scavenge Garbage Collection cycle is active and the source and destination memory regions for arraycopy overlap. This allows read and write to addresses beyond the end of the array range.	5.3	More Details
CVE-2021-47467	In the Linux kernel, the following vulnerability has been resolved: kunit: fix reference count leak in kfree_at_end The reference counting issue happens in the normal path of kfree_at_end(). When kunit_alloc_and_get_resource() is invoked, the function forgets to handle the returned resource object, whose refcount increased inside, causing a refcount leak. Fix this issue by calling kunit_alloc_resource() instead of kunit_alloc_and_get_resource(). Fixed the following when applying: Shuah Khan <skhan@linuxfoundation.org> CHECK: Alignment should match open parenthesis + kunit_alloc_resource(test, NULL, kfree_res_free, GFP_KERNEL, (void *)to_free);	5.3	More Details
CVE-2024-4858	The Testimonial Carousel For Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_testimonials_option_callback' function in versions up to, and including, 10.2.0. This makes it possible for unauthenticated attackers to update the OpenAI API key, disabling the feature.	5.3	More Details
CVE-2024-34930	A SQL injection vulnerability in /model/all_events1.php in Campcodes Complete Web-Based School Management System 1.0 allows attacker to execute arbitrary SQL commands via the month parameter.	5.3	More Details
CVE-2024-35400	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a stack overflow via the desc parameter in the function SetPortForwardRules	5.3	More Details
CVE-2024-31617	OpenLiteSpeed before 1.8.1 mishandles chunked encoding.	5.3	More Details
CVE-2024-27310	Zoho ManageEngine ADSelfService Plus versions below 6401 are vulnerable to the DOS attack due to the malicious LDAP input.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35238	Minder by Stacklok is an open source software supply chain security platform. Minder prior to version 0.0.51 is vulnerable to a denial-of-service (DoS) attack which could allow an attacker to crash the Minder server and deny other users access to it. The root cause of the vulnerability is that Minders sigstore verifier reads an untrusted response entirely into memory without enforcing a limit on the response body. An attacker can exploit this by making Minder make a request to an attacker-controlled endpoint which returns a response with a large body which will crash the Minder server. Specifically, the point of failure is where Minder parses the response from the GitHub attestations endpoint in `getAttestationReply`. Here, Minder makes a request to the `orgs/$owner/attestations/$checksumref` GitHub endpoint (line 285) and then parses the response into the `AttestationReply` (line 295). The way Minder parses the response on line 295 makes it prone to DoS if the response is large enough. Essentially, the response needs to be larger than the machine has available memory. Version 0.0.51 contains a patch for this issue. The content that is hosted at the `orgs/$owner/attestations/$checksumref` GitHub attestation endpoint is controlled by users including unauthenticated users to Minders threat model. However, a user will need to configure their own Minder settings to cause Minder to make Minder send a request to fetch the attestations. The user would need to know of a package whose attestations were configured in such a way that they would return a large response when fetching them. As such, the steps needed to carry out this attack would look as such: 1. The attacker adds a package to ghcr.io with attestations that can be fetched via the `orgs/$owner/attestations/$checksumref` GitHub endpoint. 2. The attacker registers on Minder and makes Minder fetch the attestations. 3. Minder fetches attestations and crashes thereby being denied of service.	5.3	More Details
CVE-2024-3927	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Form Submission Admin Email Bypass in all versions up to, and including, 5.6.3. This is due to the plugin not properly checking for all variations of an administrators emails. This makes it possible for unauthenticated attackers to bypass the restriction using a +value when submitting the contact form.	5.3	More Details
CVE-2024-36105	dbt enables data analysts and engineers to transform their data using the same practices that software engineers use to build applications. Prior to versions 1.6.15, 1.7.15, and 1.8.1, Binding to `INADDR_ANY (0.0.0.0)` or `IN6ADDR_ANY (::)` exposes an application on all network interfaces, increasing the risk of unauthorized access. As stated in the Python docs, a special form for address is accepted instead of a host address: `''` represents `INADDR_ANY`, equivalent to `"0.0.0.0"`. On systems with IPv6, '' represents `IN6ADDR_ANY`, which is equivalent to `"::"`. A user who serves docs on an unsecured public network, may unknowingly be hosting an unsecured (http) web site for any remote user/system to access on the same network. The issue has has been mitigated in dbt-core v1.6.15, dbt-core v1.7.15, and dbt-core v1.8.1 by binding to localhost explicitly by default in `dbt docs serve`.	5.3	More Details
CVE-2020-35165	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Observable Timing Discrepancy Vulnerability.	5.1	More Details
CVE-2024-0451	The AI ChatBot plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the openai_file_list_callback function in all versions up to, and including, 5.3.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to list files existing in a linked OpenAI account.	5.0	More Details
CVE-2024-0452	The AI ChatBot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the openai_file_upload_callback function in all versions up to, and including, 5.3.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload files to a linked OpenAI account.	5.0	More Details
CVE-2024-0453	The AI ChatBot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the openai_file_delete_callback function in all versions up to, and including, 5.3.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete files from a linked OpenAI account.	5.0	More Details
CVE-2023-6844	The iframe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to and including 5.0 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.	5.0	More Details
CVE-2024-4529	The Business Card WordPress plugin through 1.0.0 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions such as deleting card categories via CSRF attacks	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20355	A vulnerability in the implementation of SAML 2.0 single sign-on (SSO) for remote access VPN services in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to successfully establish a VPN session on an affected device. This vulnerability is due to improper separation of authorization domains when using SAML authentication. An attacker could exploit this vulnerability by using valid credentials to successfully authenticate using their designated connection profile (tunnel group), intercepting the SAML SSO token that is sent back from the Cisco ASA device, and then submitting the same SAML SSO token to a different tunnel group for authentication. A successful exploit could allow the attacker to establish a remote access VPN session using a connection profile that they are not authorized to use and connect to secured networks behind the affected device that they are not authorized to access. For successful exploitation, the attacker must have valid remote access VPN user credentials.	5.0	More Details
CVE-2024-28793	IBM Engineering Workflow Management 7.0.2 and 7.0.3 is vulnerable to stored cross-site scripting. Under certain configurations, this vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 286830.	4.9	More Details
CVE-2024-33470	An issue in the SMTP Email Settings of AVTECH Room Alert 4E v4.4.0 allows attackers to gain access to credentials in plaintext via a passback attack. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	4.9	More Details
CVE-2024-31340	TP-Link Tether versions prior to 4.5.13 and TP-Link Tapo versions prior to 3.3.6 do not properly validate certificates, which may allow a remote unauthenticated attacker to eavesdrop on an encrypted communication via a man-in-the-middle attack.	4.8	More Details
CVE-2024-35236	Audiobookshelf is a self-hosted audiobook and podcast server. Prior to version 2.10.0, opening an ebook with malicious scripts inside leads to code execution inside the browsing context. Attacking a user with high privileges (upload, creation of libraries) can lead to remote code execution (RCE) in the worst case. This was tested on version 2.9.0 on Windows, but an arbitrary file write is powerful enough as is and should easily lead to RCE on Linux, too. Version 2.10.0 contains a patch for the vulnerability.	4.8	More Details
CVE-2023-37411	IBM Aspera Faspex 5.0.0 through 5.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 260139.	4.8	More Details
CVE-2024-5194	A vulnerability was found in Arris VAP2500 08.50. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /assoc_table.php. The manipulation of the argument id leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-265831.	4.7	More Details
CVE-2024-5340	A vulnerability was found in Ruijie RG-UAC up to 20240516. It has been rated as critical. Affected by this issue is some unknown functionality of the file /view/vpn/autovpn/sub_commit.php. The manipulation of the argument key leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-266246 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-4895	The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the CSV import functionality in all versions up to, and including, 3.4.2.12 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.	4.7	More Details
CVE-2024-5241	A vulnerability was found in Huashi Private Cloud CDN Live Streaming Acceleration Server up to 20240520. It has been classified as critical. Affected is an unknown function of the file /manager/ipconfig_new.php. The manipulation of the argument dev leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-265992.	4.7	More Details
CVE-2024-5336	A vulnerability has been found in Ruijie RG-UAC up to 20240516 and classified as critical. This vulnerability affects the function addVlan of the file /view/networkConfig/vlan/vlan_add_commit.php. The manipulation of the argument phyport leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-266242 is the identifier assigned to this vulnerability. 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-2024-5337	A vulnerability was found in Ruijie RG-UAC up to 20240516 and classified as critical. This issue affects some unknown processing of the file /view/systemConfig/sys_user/user_commit.php. The manipulation of the argument email2/user_name leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266243. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-5196	A vulnerability classified as critical has been found in Arris VAP2500 08.50. This affects an unknown part of the file /tools_command.php. The manipulation of the argument cmb_header/txt_command leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-265833 was assigned to this vulnerability.	4.7	More Details
CVE-2024-35297	Cross-site scripting vulnerability exists in WP Booking versions prior to 2.4.5. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who is accessing the web site using the product.	4.7	More Details
CVE-2024-35511	phpgurukul Men Salon Management System v2.0 is vulnerable to SQL Injection via the "username" parameter of /msms/admin/index.php.	4.7	More Details
CVE-2024-21791	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL Injection in lockout history option. Note: Non-admin users cannot exploit this vulnerability.	4.7	More Details
CVE-2024-5338	A vulnerability was found in Ruijie RG-UAC up to 20240516. It has been classified as critical. Affected is an unknown function of the file /view/vpn/autovpn/online.php. The manipulation of the argument peernode leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266244. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-5195	A vulnerability was found in Arris VAP2500 08.50. It has been rated as critical. Affected by this issue is some unknown functionality of the file /diag_s.php. The manipulation of the argument customer_info leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-265832.	4.7	More Details
CVE-2024-5339	A vulnerability was found in Ruijie RG-UAC up to 20240516. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /view/vpn/autovpn/online_check.php. The manipulation of the argument peernode leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266245 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-35342	Certain Anpviz products allow unauthenticated users to modify or disable camera related settings such as microphone volume, speaker volume, LED lighting, NTP, motion detection, etc. This affects IPC-D250, IPC-D260, IPC-B850, IPC-D850, IPC-D350, IPC-D3150, IPC-D4250, IPC-D380, IPC-D880, IPC-D280, IPC-D3180, MC800N, YM500L, YM800N_N2, YMF50B, YM800SV2, YM500L8, and YM200E10 firmware v3.2.2.2 and lower and possibly more vendors/models of IP camera.	4.6	More Details
CVE-2021-47476	In the Linux kernel, the following vulnerability has been resolved: comedi: ni_usb6501: fix NULL-deref in command paths The driver uses endpoint-sized USB transfer buffers but had no sanity checks on the sizes. This can lead to zero-size-pointer dereferences or overflowed transfer buffers in ni6501_port_command() and ni6501_counter_command() if a (malicious) device has smaller max-packet sizes than expected (or when doing descriptor fuzz testing). Add the missing sanity checks to probe().	4.6	More Details
CVE-2024-3065	The PayPal Pay Now, Buy Now, Donation and Cart Buttons Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-30420	Server-side request forgery (SSRF) vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.12 and Ver.3.0.x series versions prior to Ver.3.0.32. If this vulnerability is exploited, a user with an administrator or higher privilege who can log in to the product may obtain arbitrary files on the server and information on the internal server that is not disclosed to the public.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5258	An authorization vulnerability exists within GitLab from versions 16.10 before 16.10.6, 16.11 before 16.11.3, and 17.0 before 17.0.1 where an authenticated attacker could utilize a crafted naming convention to bypass pipeline authorization logic.	4.4	More Details
CVE-2021-47555	In the Linux kernel, the following vulnerability has been resolved: net: vlan: fix underflow for the real_dev refcnt Inject error before dev_hold(real_dev) in register_vlan_dev(), and execute the following testcase: ip link add dev dummy1 type dummy ip link add name dummy1.100 link dummy1 type vlan id 100 ip link del dev dummy1 When the dummy netdevice is removed, we will get a WARNING as following: ========== refcount_t: decrement hit 0; leaking memory. WARNING: CPU: 2 PID: 0 at lib/refcount.c:31 refcount_warn_saturate+0xbf/0x1e0 and an endless loop of: ========== unregister_netdevice: waiting for dummy1 to become free. Usage count = -1073741824 That is because dev_put(real_dev) in vlan_dev_free() be called without dev_hold(real_dev) in register_vlan_dev(). It makes the refcnt of real_dev underflow. Move the dev_hold(real_dev) to vlan_dev_init() which is the call-back of ndo_init(). That makes dev_hold() and dev_put() for vlan's real_dev symmetrical.	4.4	More Details
CVE-2024-0632	The Automatic Translator with Google Translate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom font setting in all versions up to, and including, 1.5.4 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.	4.4	More Details
CVE-2023-6487	The LuckyWP Table of Contents plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Header Title' field in all versions up to and including 2.1.4 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.	4.4	More Details
CVE-2021-47547	In the Linux kernel, the following vulnerability has been resolved: net: tulip: de4x5: fix the problem that the array 'lp->phy[8]' may be out of bound In line 5001, if all id in the array 'lp->phy[8]' is not 0, when the 'for' end, the 'k' is 8. At this time, the array 'lp->phy[8]' may be out of bound.	4.4	More Details
CVE-2024-34152	Mattermost versions 9.5.x <= 9.5.3, 9.6.x <= 9.6.1 and 8.1.x <= 8.1.12 fail to perform proper access control which allows a guest to get the metadata of a public playbook run that linked to the channel they are guest via sending an RHSRuns GraphQL query request to the server	4.3	More Details
CVE-2024-5428	A vulnerability classified as problematic was found in SourceCodester Simple Online Bidding System 1.0. Affected by this vulnerability is the function save_product of the file /admin/index.php?page=manage_product of the component HTTP POST Request Handler. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-266383.	4.3	More Details
CVE-2024-29215	Mattermost versions 9.5.x <= 9.5.3, 9.7.x <= 9.7.1, 9.6.x <= 9.6.1, 8.1.x <= 8.1.12 fail to enforce proper access control which allows a user to run a slash command in a channel they are not a member of via linking a playbook run to that channel and running a slash command as a playbook task command.	4.3	More Details
CVE-2024-31859	Mattermost versions 9.5.x <= 9.5.3, 9.6.x <= 9.6.1 and 8.1.x <= 8.1.12 fail to perform proper authorization checks which allows a member running a playbook in an existing channel to be promoted to a channel admin	4.3	More Details
CVE-2024-3663	The WP Scraper plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wp_scraper_multi_scrape_action() function in all versions up to, and including, 5.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary pages and posts.	4.3	More Details
CVE-2024-34029	Mattermost versions 9.5.x <= 9.5.3, 9.7.x <= 9.7.1 and 8.1.x <= 8.1.12 fail to perform a proper authorization check in the /api/v4/groups/<group-id>/channels/<channel-id>/link endpoint which allows a user to learn the members of an AD/LDAP group that is linked to a team by adding the group to a channel, even if the user has no access to the team.	4.3	More Details
CVE-2024-4409	The WP-ViperGB plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6.1. This is due to missing or incorrect nonce validation when saving plugin settings. This makes it possible for unauthenticated attackers to change the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5273	Jenkins Report Info Plugin 1.2 and earlier does not perform path validation of the workspace directory while serving report files, allowing attackers with Item/Configure permission to retrieve Surefire failures, PMD violations, Findbugs bugs, and Checkstyle errors on the controller file system by editing the workspace path.	4.3	More Details
CVE-2024-24584	Multiple out-of-bounds read vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds read. An attacker can provide a malicious file to trigger this vulnerability.This vulnerabilitty concerns the`readMSH` function while processing `MshLoader::ELEMENT_TET` elements.	4.3	More Details
CVE-2024-5270	Mattermost versions 9.5.x <= 9.5.3, 9.7.x <= 9.7.1, 9.6.x <= 9.6.1 and 8.1.x <= 8.1.12 fail to check if the email signup configuration option is enabled when a user requests to switch from SAML to Email. This allows the user to switch their authentication mail from SAML to email and possibly edit personal details that were otherwise non-editable and provided by the SAML provider.	4.3	More Details
CVE-2024-5272	Mattermost versions 9.5.x <= 9.5.3, 9.6.x <= 9.6.1, 8.1.x <= 8.1.12 fail to restrict the audience of the "custom_playbooks_playbook_run_updated" webhook event, which allows a guest on a channel with a playbook run linked to see all the details of the playbook run when the run is marked by finished.	4.3	More Details
CVE-2024-31893	IBM App Connect Enterprise 12.0.1.0 through 12.0.12.1 could allow an authenticated user to obtain sensitive calendar information using an expired access token. IBM X-Force ID: 288174.	4.3	More Details
CVE-2024-24583	Multiple out-of-bounds read vulnerabilities exist in the readMSH functionality of libigl v2.5.0. A specially crafted .msh file can lead to an out-of-bounds read. An attacker can provide a malicious file to trigger this vulnerability.This vulnerabilitty concerns the`readMSH` function while processing `MshLoader::ELEMENT_TRI` elements.	4.3	More Details
CVE-2024-31894	IBM App Connect Enterprise 12.0.1.0 through 12.0.12.1 could allow an authenticated user to obtain sensitive user information using an expired access token. IBM X-Force ID: 288175.	4.3	More Details
CVE-2024-31895	IBM App Connect Enterprise 12.0.1.0 through 12.0.12.1 could allow an authenticated user to obtain sensitive user information using an expired access token. IBM X-Force ID: 288176.	4.3	More Details
CVE-2024-2036	The ApplyOnline – Application Form Builder and Manager plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the aol_modal_box AJAX action in all versions up to, and including, 2.6. This makes it possible for authenticated attackers, with subscriber access or higher, to view Application submissions.	4.3	More Details
CVE-2024-34995	svnWebUI v1.8.3 was discovered to contain an arbitrary file deletion vulnerability via the dirTemps parameter under com.cym.controller.UserController#importOver. This vulnerability allows attackers to delete arbitrary files via a crafted POST request.	4.3	More Details
CVE-2024-1947	A denial of service (DoS) condition was discovered in GitLab CE/EE affecting all versions from 13.2.4 before 16.10.6, 16.11 before 16.11.3, and 17.0 before 17.0.1. By leveraging this vulnerability an attacker could create a DoS condition by sending crafted API calls.	4.3	More Details
CVE-2024-0893	The Schema App Structured Data plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the MarkupUpdate function in all versions up to, and including, 2.1.0. This makes it possible for authenticated attackers, with subscriber access or higher, to update or delete post metadata.	4.3	More Details
CVE-2024-1376	The Event post plugin for WordPress is vulnerable to unauthorized bulk metadata update due to a missing capability check on the save_bulkdatas function in all versions up to, and including, 5.9.4. This makes it possible for authenticated attackers, with subscriber access or higher, to update post_meta_data.	4.3	More Details
CVE-2023-6502	A Denial of Service (DoS) condition has been discovered in GitLab CE/EE affecting all versions before 16.10.6, version 16.11 before 16.11.3, and 17.0 before 17.0.1. It is possible for an attacker to cause a denial of service using a crafted wiki page.	4.3	More Details
CVE-2023-46442	An infinite loop in the retrieveActiveBody function of Soot before v4.4.1 under Java 8 allows attackers to cause a Denial of Service (DoS).	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3711	The Brizy – Page Builder plugin for WordPress is vulnerable to unauthorized plugin setting update due to a missing capability check on the functions action_request_disable, action_change_template, and action_request_enable in all versions up to, and including, 2.4.43. This makes it possible for authenticated attackers, with contributor access or above, to enable/disable the Brizy editor and modify the template used.	4.3	More Details
CVE-2023-30306	An issue discovered in Mercury x30g, Mercury YR1800XG routers allows attackers to hijack TCP sessions which could lead to a denial of service.	4.3	More Details
CVE-2024-3626	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_template_content function in all versions up to, and including, 5.7.17. This makes it possible for authenticated attackers, with subscriber access and above, to obtain the contents of private and password-protected posts.	4.3	More Details
CVE-2024-5354	A vulnerability classified as problematic was found in anji-plus AJ-Report up to 1.4.1. This vulnerability affects unknown code of the file /reportShare/detailByCode. The manipulation of the argument shareToken leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-266266 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2024-1803	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to unauthorized access of functionality due to insufficient authorization validation on the PDF embed block in all versions up to, and including, 3.9.12. This makes it possible for authenticated attackers, with contributor-level access and above, to embed PDF blocks.	4.3	More Details
CVE-2024-36036	Zoho ManageEngine ADAudit Plus versions 7260 and below allows unauthorized local agent machine users to access sensitive information and modifying the agent configuration.	4.2	More Details
CVE-2021-47534	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: kms: Add missing drm_crtc_commit_put Commit 9ec03d7f1ed3 ("drm/vc4: kms: Wait on previous FIFO users before a commit") introduced a global state for the HVS, with each FIFO storing the current CRTC commit so that we can properly synchronize commits. However, the refcounting was off and we thus ended up leaking the drm_crtc_commit structure every commit. Add a drm_crtc_commit_put to prevent the leakage.	4.1	More Details
CVE-2024-31843	An issue was discovered in Italtel Embrace 1.6.4. The Web application does not properly check the parameters sent as input before they are processed on the server side. This allows authenticated users to execute commands on the Operating System.	4.1	More Details
CVE-2024-5318	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.11 prior to 16.10.6, starting from 16.11 prior to 16.11.3, and starting from 17.0 prior to 17.0.1. A Guest user can view dependency lists of private projects through job artifacts.	4.0	More Details
CVE-2024-35232	github.com/huandu/facebook is a Go package that fully supports the Facebook Graph API with file upload, batch request and marketing API. access_token can be exposed in error message on fail in HTTP request. This issue has been patched in version 2.7.2.	3.7	More Details
CVE-2024-5376	A vulnerability was found in Kashipara College Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file view_each_faculty.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266288.	3.5	More Details
CVE-2024-5380	A vulnerability classified as problematic has been found in jsy-1 short-url 1.0.0. Affected is an unknown function of the file admin.php. The manipulation of the argument url leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.0.0 is able to address this issue. The name of the patch is 35c790897d6979392bc6f60707fc32da13a98b63. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-266292.	3.5	More Details
CVE-2024-5379	A vulnerability was found in JFinalCMS up to 20240111. It has been rated as problematic. This issue affects some unknown processing of the file /admin/template. The manipulation of the argument directory leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266291.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5374	A vulnerability, which was classified as problematic, was found in Kashipara College Management System 1.0. Affected is an unknown function of the file submit_new_faculty.php. The manipulation of the argument address 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. VDB-266286 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-5383	A vulnerability classified as problematic has been found in lakernote EasyAdmin up to 20240324. This affects an unknown part of the file /sys/file/upload. The manipulation of the argument file leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 9c8a836ace17a93c45e5ad52a2340788b7795030. It is recommended to apply a patch to fix this issue. The identifier VDB-266301 was assigned to this vulnerability.	3.5	More Details
CVE-2024-5375	A vulnerability has been found in Kashipara College Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file submit_student.php. The manipulation of the argument address leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266287.	3.5	More Details
CVE-2024-5371	A vulnerability classified as problematic has been found in Kashipara College Management System 1.0. This affects an unknown part of the file submit_enroll_student.php. The manipulation of the argument class_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. The associated identifier of this vulnerability is VDB-266283.	3.5	More Details
CVE-2024-5373	A vulnerability, which was classified as problematic, has been found in Kashipara College Management System 1.0. This issue affects some unknown processing of the file submit_login.php. The manipulation of the argument usertype leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266285 was assigned to this vulnerability.	3.5	More Details
CVE-2024-3920	The Flattr WordPress plugin through 1.2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	3.5	More Details
CVE-2024-2220	The Button contact VR WordPress plugin through 4.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	3.5	More Details
CVE-2024-5279	A vulnerability was found in Qiwen Netdisk up to 1.4.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component File Rename Handler. The manipulation with the input <img src="" onerror="alert(document.cookie)"> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266083.	3.5	More Details
CVE-2024-5372	A vulnerability classified as problematic was found in Kashipara College Management System 1.0. This vulnerability affects unknown code of the file submit_extracurricular_activity.php. The manipulation of the argument activity_contact leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266284.	3.5	More Details
CVE-2023-1001	A vulnerability, which was classified as problematic, has been found in xuliangzhan vxe-table up to 3.7.9. This issue affects the function export of the file packages/textarea/src/textarea.js of the component vxe-textarea. The manipulation of the argument inputValue leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 3.7.10 is able to address this issue. The patch is named d70b0e089740b65a22c89c106ebc4627ac48a22d. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-266123.	3.5	More Details
CVE-2024-5367	A vulnerability was found in Kashipara College Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file each_extracurricula_activities.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-266279.	3.5	More Details
CVE-2024-5368	A vulnerability was found in Kashipara College Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file delete_faculty.php. The manipulation of the argument id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-266280.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5370	A vulnerability was found in Kashipara College Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file submit_enroll_staff.php. The manipulation of the argument class_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-266282 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-5369	A vulnerability was found in Kashipara College Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file submit_admin.php. The manipulation of the argument admin_name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-266281 was assigned to this vulnerability.	3.5	More Details
CVE-2024-32944	Path traversal vulnerability exists in UTAU versions prior to v0.4.19. If a user of the product installs a crafted UTAU voicebank installer (.uar file, .zip file) to UTAU, an arbitrary file may be placed.	3.3	More Details
CVE-2024-36241	Mattermost versions 9.5.x <= 9.5.3, 9.6.x <= 9.6.1 and 8.1.x <= 8.1.12 fail to enforce proper access controls which allows user to view arbitrary post contents via the /playbook add slash command	3.1	More Details
CVE-2024-32969	vantage6 is an open-source infrastructure for privacy preserving analysis. Collaboration administrators can add extra organizations to their collaboration that can extend their influence. For example, organizations that they include can then create new users for which they know the passwords, and use that to read task results of other collaborations that that organization is involved in. This is only relatively trusted users - with access to manage a collaboration - are able to do this, which reduces the impact. This vulnerability was patched in version 4.5.0rc3.	2.7	More Details
CVE-2024-35403	TOTOLINK CP900L v4.1.5cu.798_B20221228 was discovered to contain a stack overflow via the desc parameter in the function setIpPortFilterRules	2.7	More Details
CVE-2024-35239	Umbraco Commerce is an open source dotnet web forms solution. In affected versions an authenticated user that has access to edit Forms may inject unsafe code into Forms components. This issue can be mitigated by configuring TitleAndDescription:AllowUnsafeHtmlRendering after upgrading to one of the patched versions (13.0.1, 12.2.2, 10.5.3, 8.13.13).	2.7	More Details
CVE-2024-5310	A vulnerability classified as problematic has been found in JFinalCMS up to 20221020. This affects an unknown part of the file /admin/content. The manipulation of the argument Title 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. The identifier VDB-266121 was assigned to this vulnerability.	2.4	More Details
CVE-2024-27314	Zoho ManageEngine ServiceDesk Plus versions below 14730, ServiceDesk Plus MSP below 14720 and SupportCenter Plus below 14720 are vulnerable to stored XSS in the Custom Actions menu on the request details. This vulnerability can be exploited only by the SDAdmin role users.	2.4	More Details
CVE-2024-5385	A vulnerability, which was classified as problematic, has been found in oretnom23 Online Car Wash Booking System 1.0. This issue affects some unknown processing of the file /admin/?page=user/list. The manipulation of the argument First Name/Last Name with the input <script>confirm (document.cookie)</script> leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-266303.	2.4	More Details
CVE-2023-7259	** DISPUTED ** A vulnerability was found in zzdevelop lenosp up to 20230831. It has been classified as problematic. This affects an unknown part of the component Adduser Page. The manipulation of the argument username with the input <script>alert(1)</script> 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. The real existence of this vulnerability is still doubted at the moment. The associated identifier of this vulnerability is VDB-266127. NOTE: The vendor rejected the issue because he claims that XSS which require administrative privileges are not of any use for attackers.	2.4	More Details
CVE-2023-1111	A vulnerability was found in FastCMS up to 0.1.5 and classified as problematic. Affected by this issue is some unknown functionality of the component New Article Tab. The manipulation of the argument Title leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-266126 is the identifier assigned to this vulnerability.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47440	In the Linux kernel, the following vulnerability has been resolved: net: encx24j600: check error in devm_regmap_init_encx24j600 devm_regmap_init may return error which caused by like out of memory, this will results in null pointer dereference later when reading or writing register: general protection fault in encx24j600_spi_probe KASAN: null-ptr-deref in range [0x0000000000000090-0x0000000000000097] CPU: 0 PID: 286 Comm: spi-encx24j600- Not tainted 5.15.0-rc2-00142-g9978db750e31-dirty #11 9c53a778c1306b1b02359f3c2bbedc0222cba652 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 RIP: 0010:regcache_cache_bypass drivers/base/regmap/regcache.c:540 Code: 54 41 89 f4 55 53 48 89 fb 48 83 ec 08 e8 26 94 a8 fe 48 8d bb a0 00 00 00 48 b8 00 00 00 00 00 fc ff df 48 89 fa 48 c1 ea 03 <80> 3c 02 00 0f 85 4a 03 00 00 4c 8d ab b0 00 00 00 48 8b ab a0 00 RSP: 0018:ffffc900010476b8 EFLAGS: 00010207 RAX: dfffc0000000000 RBX: fffffffffffffff4 RCX: 0000000000000000 RDX: 0000000000000012 RSI: ffff888002de0000 RDI: 0000000000000094 RBP: ffff888013c9a000 R08: 0000000000000000 R09: fffffbfff3f9cc6a R10: ffffc900010476e8 R11: fffffbfff3f9cc69 R12: 0000000000000001 R13: 000000000000000a R14: ffff888013c9af54 R15: ffff888013c9ad08 FS: 00007ffa984ab580(0000) GS:ffff88801fe00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055a6384136c8 CR3: 000000003bbe6003 CR4: 0000000000770ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: encx24j600_spi_probe drivers/net/ethernet/microchip/encx24j600.c:459 spi_probe drivers/spi/spi.c:397 really_probe drivers/base/dd.c:517 __driver_probe_device drivers/base/dd.c:751 driver_probe_device drivers/base/dd.c:782 __device_attach_driver drivers/base/dd.c:899 bus_for_each_drv drivers/base/bus.c:427 __device_attach drivers/base/dd.c:971 bus_probe_device drivers/base/bus.c:487 device_add drivers/base/core.c:3364 __spi_add_device drivers/spi/spi.c:599 spi_add_device drivers/spi/spi.c:641 spi_new_device drivers/spi/spi.c:717 new_device_store+0x18c/0x1f1 [spi_stub 4e02719357f1ff33f5a43d00630982840568e85e] dev_attr_store drivers/base/core.c:2074 sysfs_kf_write fs/sysfs/file.c:139 kernfs_fop_write_iter fs/kernfs/file.c:300 new_sync_write fs/read_write.c:508 (discriminator 4) vfs_write fs/read_write.c:594 ksys_write fs/read_write.c:648 do_syscall_64 arch/x86/entry/common.c:50 entry_SYSCALL_64_after_hwframe arch/x86/entry/entry_64.S:113 Add error check in devm_regmap_init_encx24j600 to avoid this situation.	2.3	More Details
CVE-2021-47455	In the Linux kernel, the following vulnerability has been resolved: ptp: Fix possible memory leak in ptp_clock_register() I got memory leak as follows when doing fault injection test: unreferenced object 0xffff88800906c618 (size 8): comm "i2c-idt82p33931", pid 4421, jiffies 4294948083 (age 13.188s) hex dump (first 8 bytes): 70 74 70 30 00 00 00 00 ptp0.... backtrace: [<00000000312ed458>] __kmalloc_track_caller+0x19f/0x3a0 [<0000000079f6e2ff>] kvasprintf+0xb5/0x150 [<0000000026aae54f>] kvasprintf_const+0x60/0x190 [<00000000f323a5f7>] kobject_set_name_vargs+0x56/0x150 [<000000004e35abdd>] dev_set_name+0xc0/0x100 [<00000000f20cfe25>] ptp_clock_register+0x9f4/0xd30 [ptp] [<000000008bb9f0de>] idt82p33_probe.cold+0x8b6/0x1561 [ptp_idt82p33] When posix_clock_register() returns an error, the name allocated in dev_set_name() will be leaked, the put_device() should be used to give up the device reference, then the name will be freed in kobject_cleanup() and other memory will be freed in ptp_clock_release().	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47462	In the Linux kernel, the following vulnerability has been resolved: mm/mempolicy: do not allow illegal MPOL_F_NUMA_BALANCING | MPOL_LOCAL in mbind() syzbot reported access to unitialized memory in mbind() [1] Issue came with commit bda420b98505 ("numa balancing: migrate on fault among multiple bound nodes") This commit added a new bit in MPOL_MODE_FLAGS, but only checked valid combination (MPOL_F_NUMA_BALANCING can only be used with MPOL_BIND) in do_set_mempolicy() This patch moves the check in sanitize_mpol_flags() so that it is also used by mbind() [1] BUG: KMSAN: uninit-value in __mpol_equal+0x567/0x590 mm/mempolicy.c:2260 __mpol_equal+0x567/0x590 mm/mempolicy.c:2260 mpol_equal include/linux/mempolicy.h:105 [inline] vma_merge+0x4a1/0x1e60 mm/mmap.c:1190 mbind_range+0xcc8/0x1e80 mm/mempolicy.c:811 do_mbind+0xf42/0x15f0 mm/mempolicy.c:1333 kernel_mbind mm/mempolicy.c:1483 [inline] __do_sys_mbind mm/mempolicy.c:1490 [inline] __se_sys_mbind+0x437/0xb80 mm/mempolicy.c:1486 __x64_sys_mbind+0x19d/0x200 mm/mempolicy.c:1486 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_alloc_node mm/slub.c:3221 [inline] slab_alloc mm/slub.c:3230 [inline] kmem_cache_alloc+0x751/0xff0 mm/slub.c:3235 mpol_new mm/mempolicy.c:293 [inline] do_mbind+0x912/0x15f0 mm/mempolicy.c:1289 kernel_mbind mm/mempolicy.c:1483 [inline] __do_sys_mbind mm/mempolicy.c:1490 [inline] __se_sys_mbind+0x437/0xb80 mm/mempolicy.c:1486 __x64_sys_mbind+0x19d/0x200 mm/mempolicy.c:1486 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae === Kernel panic - not syncing: panic_on_kmsan set ... CPU: 0 PID: 15049 Comm: syz-executor.0 Tainted: G B 5.15.0-rc2-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1ff/0x28e lib/dump_stack.c:106 dump_stack+0x25/0x28 lib/dump_stack.c:113 panic+0x44f/0xdeb kernel/panic.c:232 kmsan_report+0x2ee/0x300 mm/kmsan/report.c:186 __msan_warning+0xd7/0x150 mm/kmsan/instrumentation.c:208 __mpol_equal+0x567/0x590 mm/mempolicy.c:2260 mpol_equal include/linux/mempolicy.h:105 [inline] vma_merge+0x4a1/0x1e60 mm/mmap.c:1190 mbind_range+0xcc8/0x1e80 mm/mempolicy.c:811 do_mbind+0xf42/0x15f0 mm/mempolicy.c:1333 kernel_mbind mm/mempolicy.c:1483 [inline] __do_sys_mbind mm/mempolicy.c:1490 [inline] __se_sys_mbind+0x437/0xb80 mm/mempolicy.c:1486 __x64_sys_mbind+0x19d/0x200 mm/mempolicy.c:1486 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae	N/A	More Details
CVE-2021-47457	In the Linux kernel, the following vulnerability has been resolved: can: isotp: isotp_sendmsg(): add result check for wait_event_interruptible() Using wait_event_interruptible() to wait for complete transmission, but do not check the result of wait_event_interruptible() which can be interrupted. It will result in TX buffer has multiple accessors and the later process interferes with the previous process. Following is one of the problems reported by syzbot. == WARNING: CPU: 0 PID: 0 at net/can/isotp.c:840 isotp_tx_timer_handler+0x2e0/0x4c0 CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.13.0-rc7+ #68 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1 04/01/2014 RIP: 0010:isotp_tx_timer_handler+0x2e0/0x4c0 Call Trace: <IRQ> ? isotp_setsockopt+0x390/0x390 __hrtimer_run_queues+0xb8/0x610 hrtimer_run_softirq+0x91/0xd0 ? rcu_read_lock_sched_held+0x4d/0x80 __do_softirq+0xe8/0x553 irq_exit_rcu+0xf8/0x100 sysvec_apic_timer_interrupt+0x9e/0xc0 </IRQ> asm_sysvec_apic_timer_interrupt+0x12/0x20 Add result check for wait_event_interruptible() in isotp_sendmsg() to avoid multiple accessers for tx buffer.	N/A	More Details
CVE-2021-47454	In the Linux kernel, the following vulnerability has been resolved: powerpc/smp: do not decrement idle task preempt count in CPU offline With PREEMPT_COUNT=y, when a CPU is offlined and then onlined again, we get: BUG: scheduling while atomic: swapper/1/0/0x00000000 no locks held by swapper/1/0. CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.15.0-rc2+ #100 Call Trace: dump_stack_lvl+0xac/0x108 __schedule_bug+0xac/0xe0 __schedule+0xcf8/0x10d0 schedule_idle+0x3c/0x70 do_idle+0x2d8/0x4a0 cpu_startup_entry+0x38/0x40 start_secondary+0x2ec/0x3a0 start_secondary_prolog+0x10/0x14 This is because powerpc's arch_cpu_idle_dead() decrements the idle task's preempt count, for reasons explained in commit a7c2bb8279d2 ("powerpc: Re-enable preemption before cpu_die()"), specifically "start_secondary() expects a preempt_count() of 0." However, since commit 2c669ef6979c ("powerpc/preempt: Don't touch the idle task's preempt_count during hotplug") and commit f1a0a376ca0c ("sched/core: Initialize the idle task with preemption disabled"), that justification no longer holds. The idle task isn't supposed to re-enable preemption, so remove the vestigial preempt_enable() from the CPU offline path. Tested with pseries and powernv in qemu, and pseries on PowerVM.	N/A	More Details
CVE-2024-30212	If a SCSI READ(10) command is initiated via USB using the largest LBA (0xFFFFFFFF) with it's default block size of 512 and a count of 1, the first 512 byte of the 0x80000000 memory area is returned to the user. If the block count is increased, the full RAM can be exposed. The same method works to write to this memory area. If RAM contains pointers, those can be - depending on the application - overwritten to return data from any other offset including Progam and Boot Flash.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47458	In the Linux kernel, the following vulnerability has been resolved: ocfs2: mount fails with buffer overflow in strlen Starting with kernel 5.11 built with CONFIG_FORTIFY_SOURCE mouting an ocfs2 filesystem with either o2cb or pcmk cluster stack fails with the trace below. Problem seems to be that strings for cluster stack and cluster name are not guaranteed to be null terminated in the disk representation, while strlcpy assumes that the source string is always null terminated. This causes a read outside of the source string triggering the buffer overflow detection. detected buffer overflow in strlen ------------[cut here]------------ kernel BUG at lib/string.c:1149! invalid opcode: 0000 [#1] SMP PTI CPU: 1 PID: 910 Comm: mount.ocfs2 Not tainted 5.14.0-1-amd64 #1 Debian 5.14.6-2 RIP: 0010:fortify_panic+0xf/0x11 ... Call Trace: ocfs2_initialize_super.isra.0.cold+0xc/0x18 [ocfs2] ocfs2_fill_super+0x359/0x19b0 [ocfs2] mount_bdev+0x185/0x1b0 legacy_get_tree+0x27/0x40 vfs_get_tree+0x25/0xb0 path_mount+0x454/0xa20 __x64_sys_mount+0x103/0x140 do_syscall_64+0x3b/0xc0 entry_SYSCALL_64_after_hwframe+0x44/0xae	N/A	More Details
CVE-2021-47459	In the Linux kernel, the following vulnerability has been resolved: can: j1939: j1939_netdev_start(): fix UAF for rx_kref of j1939_priv It will trigger UAF for rx_kref of j1939_priv as following. cpu0 cpu1 j1939_sk_bind(socket0, ndev0, ...) j1939_netdev_start j1939_sk_bind(socket1, ndev0, ...) j1939_netdev_start j1939_priv_set j1939_priv_get_by_ndev_locked j1939_jsk_add ..... j1939_netdev_stop kref_put_lock(&priv->rx_kref, ...) kref_get(&priv->rx_kref, ...) REFCOUNT_WARN("addition on 0;...") == refcount_t: addition on 0; use-after-free. WARNING: CPU: 1 PID: 20874 at lib/refcount.c:25 refcount_warn_saturate+0x169/0x1e0 RIP: 0010:refcount_warn_saturate+0x169/0x1e0 Call Trace: j1939_netdev_start+0x68b/0x920 j1939_sk_bind+0x426/0xeb0 ? security_socket_bind+0x83/0xb0 The rx_kref's kref_get() and kref_put() should use j1939_netdev_lock to protect.	N/A	More Details
CVE-2021-47460	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix data corruption after conversion from inline format Commit 6dbf7bb55598 ("fs: Don't invalidate page buffers in block_write_full_page()") uncovered a latent bug in ocfs2 conversion from inline inode format to a normal inode format. The code in ocfs2_convert_inline_data_to_extents() attempts to zero out the whole cluster allocated for file data by grabbing, zeroing, and dirtying all pages covering this cluster. However these pages are beyond i_size, thus writeback code generally ignores these dirty pages and no blocks were ever actually zeroed on the disk. This oversight was fixed by commit 693c241a5f6a ("ocfs2: No need to zero pages past i_size.") for standard ocfs2 write path, inline conversion path was apparently forgotten; the commit log also has a reasoning why the zeroing actually is not needed. After commit 6dbf7bb55598, things became worse as writeback code stopped invalidating buffers on pages beyond i_size and thus these pages end up with clean PageDirty bit but with buffers attached to these pages being still dirty. So when a file is converted from inline format, then writeback triggers, and then the file is grown so that these pages become valid, the invalid dirtiness state is preserved, mark_buffer_dirty() does nothing on these pages (buffers are already dirty) but page is never written back because it is clean. So data written to these pages is lost once pages are reclaimed. Simple reproducer for the problem is: xfs_io -f -c "pwrite 0 2000" -c "pwrite 2000 2000" -c "fsync" \ -c "pwrite 4000 2000" ocfs2_file After unmounting and mounting the fs again, you can observe that end of 'ocfs2_file' has lost its contents. Fix the problem by not doing the pointless zeroing during conversion from inline format similarly as in the standard write path. [akpm@linux-foundation.org: fix whitespace, per Joseph]	N/A	More Details
CVE-2024-35621	A cross-site scripting (XSS) vulnerability in the Edit function of Formwork before 1.13.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Content field.	N/A	More Details
CVE-2021-47453	In the Linux kernel, the following vulnerability has been resolved: ice: Avoid crash from unnecessary IDA free In the remove path, there is an attempt to free the aux_idx IDA whether it was allocated or not. This can potentially cause a crash when unloading the driver on systems that do not initialize support for RDMA. But, this free cannot be gated by the status bit for RDMA, since it is allocated if the driver detects support for RDMA at probe time, but the driver can enter into a state where RDMA is not supported after the IDA has been allocated at probe time and this would lead to a memory leak. Initialize aux_idx to an invalid value and check for a valid value when unloading to determine if an IDA free is necessary.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47452	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: skip netdev events generated on netns removal syzbot reported following (harmless) WARN: WARNING: CPU: 1 PID: 2648 at net/netfilter/core.c:468 nft_netdev_unregister_hooks net/netfilter/nf_tables_api.c:230 [inline] nf_tables_unregister_hook include/net/netfilter/nf_tables.h:1090 [inline] __nft_release_basechain+0x138/0x640 net/netfilter/nf_tables_api.c:9524 nft_netdev_event net/netfilter/nft_chain_filter.c:351 [inline] nf_tables_netdev_event+0x521/0x8a0 net/netfilter/nft_chain_filter.c:382 reproducer: unshare -n bash -c 'ip link add br0 type bridge; nft add table netdev t ; \ nft add chain netdev t ingress \{ type filter hook ingress device "br0" \ priority 0\; policy drop\; \}' Problem is that when netns device exit hooks create the UNREGISTER event, the .pre_exit hook for nf_tables core has already removed the base hook. Notifier attempts to do this again. The need to do base hook unregister unconditionally was needed in the past, because notifier was last stage where reg->dev dereference was safe. Now that nf_tables does the hook removal in .pre_exit, this isn't needed anymore.	N/A	More Details
CVE-2021-47461	In the Linux kernel, the following vulnerability has been resolved: userfaultfd: fix a race between writeprotect and exit_mmap() A race is possible when a process exits, its VMAs are removed by exit_mmap() and at the same time userfaultfd_writeprotect() is called. The race was detected by KASAN on a development kernel, but it appears to be possible on vanilla kernels as well. Use mmget_not_zero() to prevent the race as done in other userfaultfd operations.	N/A	More Details
CVE-2021-47469	In the Linux kernel, the following vulnerability has been resolved: spi: Fix deadlock when adding SPI controllers on SPI buses Currently we have a global spi_add_lock which we take when adding new devices so that we can check that we're not trying to reuse a chip select that's already controlled. This means that if the SPI device is itself a SPI controller and triggers the instantiation of further SPI devices we trigger a deadlock as we try to register and instantiate those devices while in the process of doing so for the parent controller and hence already holding the global spi_add_lock. Since we only care about concurrency within a single SPI bus move the lock to be per controller, avoiding the deadlock. This can be easily triggered in the case of spi-mux.	N/A	More Details
CVE-2021-47463	In the Linux kernel, the following vulnerability has been resolved: mm/secretmem: fix NULL page->mapping dereference in page_is_secretmem() Check for a NULL page->mapping before dereferencing the mapping in page_is_secretmem(), as the page's mapping can be nullified while gup() is running, e.g. by reclaim or truncation. BUG: kernel NULL pointer dereference, address: 0000000000000068 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 6 PID: 4173897 Comm: CPU 3/KVM Tainted: G W RIP: 0010:internal_get_user_pages_fast+0x621/0x9d0 Code: <48> 81 7a 68 80 08 04 bc 0f 85 21 ff ff 8 89 c7 be RSP: 0018:ffffaa90087679b0 EFLAGS: 00010046 RAX: ffffe3f37905b900 RBX: 00007f2dd561e000 RCX: ffffe3f37905b934 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffffe3f37905b900 ... CR2: 0000000000000068 CR3: 00000004c5898003 CR4: 00000000001726e0 Call Trace: get_user_pages_fast_only+0x13/0x20 hva_to_pfn+0xa9/0x3e0 try_async_pf+0xa1/0x270 direct_page_fault+0x113/0xad0 kvm_mmu_page_fault+0x69/0x680 vmx_handle_exit+0xe1/0x5d0 kvm_arch_vcpu_ioctl_run+0xd81/0x1c70 kvm_vcpu_ioctl+0x267/0x670 __x64_sys_ioctl+0x83/0xa0 do_syscall_64+0x56/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae	N/A	More Details
CVE-2021-47502	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: wcd934x: handle channel mappping list correctly Currently each channel is added as list to dai channel list, however there is danger of adding same channel to multiple dai channel list which endups corrupting the other list where its already added. This patch ensures that the channel is actually free before adding to the dai channel list and also ensures that the channel is on the list before deleting it. This check was missing previously, and we did not hit this issue as we were testing very simple usecases with sequence of amixer commands.	N/A	More Details
CVE-2021-47514	In the Linux kernel, the following vulnerability has been resolved: devlink: fix netns refcount leak in devlink_nl_cmd_reload() While preparing my patch series adding netns refcount tracking, I spotted bugs in devlink_nl_cmd_reload() Some error paths forgot to release a refcount on a netns. To fix this, we can reduce the scope of get_net()/put_net() section around the call to devlink_reload().	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47512	In the Linux kernel, the following vulnerability has been resolved: net/sched: fq_pie: prevent dismantle issue For some reason, fq_pie_destroy() did not copy working code from pie_destroy() and other qdiscs, thus causing elusive bug. Before calling del_timer_sync(&q->adapt_timer), we need to ensure timer will not rearm itself. rcu: INFO: rcu_preempt self-detected stall on CPU rcu: 0-....: (4416 ticks this GP) idle=60d/1/0x4000000000000000 softirq=10433/10434 fqs=2579 (t=10501 jiffies g=13085 q=3989) NMI backtrace for cpu 0 CPU: 0 PID: 13 Comm: ksoftirqd/0 Not tainted 5.16.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 nmi_cpu_backtrace.cold+0x47/0x144 lib/nmi_backtrace.c:111 nmi_trigger_cpumask_backtrace+0x1b3/0x230 lib/nmi_backtrace.c:62 trigger_single_cpu_backtrace include/linux/nmi.h:164 [inline] rcu_dump_cpu_stacks+0x25e/0x3f0 kernel/rcu/tree_stall.h:343 print_cpu_stall kernel/rcu/tree_stall.h:627 [inline] check_cpu_stall kernel/rcu/tree_stall.h:711 [inline] rcu_pending kernel/rcu/tree.c:3878 [inline] rcu_sched_clock_irq.cold+0x9d/0x746 kernel/rcu/tree.c:2597 update_process_times+0x16d/0x200 kernel/time/timer.c:1785 tick_sched_handle+0x9b/0x180 kernel/time/tick-sched.c:226 tick_sched_timer+0x1b0/0x2d0 kernel/time/tick-sched.c:1428 __run_hrtimer kernel/time/hrtimer.c:1685 [inline] __hrtimer_run_queues+0x1c0/0xe50 kernel/time/hrtimer.c:1749 hrtimer_interrupt+0x31c/0x790 kernel/time/hrtimer.c:1811 local_apic_timer_interrupt arch/x86/kernel/apic/apic.c:1086 [inline] __sysvec_apic_timer_interrupt+0x146/0x530 arch/x86/kernel/apic/apic.c:1103 sysvec_apic_timer_interrupt+0x8e/0xc0 arch/x86/kernel/apic/apic.c:1097 </IRQ> <TASK> asm_sysvec_apic_timer_interrupt+0x12/0x20 arch/x86/include/asm/idtentry.h:638 RIP: 0010:write_comp_data kernel/kcov.c:221 [inline] RIP: 0010:__sanitizer_cov_trace_const_cmp1+0x1d/0x80 kernel/kcov.c:273 Code: 54 c8 20 48 89 10 c3 66 0f 1f 44 00 00 53 41 89 fb 41 89 f1 bf 03 00 00 00 65 48 8b 0c 25 40 70 02 00 48 89 ce 4c 8b 54 24 08 <e8> 4e f7 ff ff 84 c0 74 51 48 8b 81 88 15 00 00 44 8b 81 84 15 00 RSP: 0018:ffffc90000d27b28 EFLAGS: 00000246 RAX: 0000000000000000 RBX: ffff888064bf1bf0 RCX: ffff888011928000 RDX: ffff888011928000 RSI: ffff888011928000 RDI: 0000000000000003 RBP: ffff888064bf1c28 R08: 0000000000000000 R09: 0000000000000000 R10: ffffffff875d8295 R11: 0000000000000000 R12: 0000000000000000 R13: ffff8880783dd300 R14: 0000000000000000 R15: 0000000000000000 pie_calculate_probability+0x405/0x7c0 net/sched/sch_pie.c:418 fq_pie_timer+0x170/0x2a0 net/sched/sch_fq_pie.c:383 call_timer_fn+0x1a5/0x6b0 kernel/time/timer.c:1421 expire_timers kernel/time/timer.c:1466 [inline] __run_timers.part.0+0x675/0xa20 kernel/time/timer.c:1734 __run_timers kernel/time/timer.c:1715 [inline] run_timer_softirq+0xb3/0x1d0 kernel/time/timer.c:1747 __do_softirq+0x29b/0x9c2 kernel/softirq.c:558 run_ksoftirqd kernel/softirq.c:921 [inline] run_ksoftirqd+0x2d/0x60 kernel/softirq.c:913 smpboot_thread_fn+0x645/0x9c0 kernel/smpboot.c:164 kthread+0x405/0x4f0 kernel/kthread.c:327 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK>	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47510	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix re-dirty process of tree-log nodes There is a report of a transaction abort of -EAGAIN with the following script. #!/bin/sh for d in sda sdb; do mkfs.btrfs -d single -m single -f /dev/\${d} done mount /dev/sda /mnt/test mount /dev/sdb /mnt/scratch for dir in test scratch; do echo 3 >/proc/sys/vm/drop_caches fio --directory=/mnt/\${dir} --name=fio.\${dir} --rw=read --size=50G --bs=64m \ --numjobs=$(nproc) --time_based --ramp_time=5 --runtime=480 \ --group_reporting |& tee /dev/shm/fio.\${dir} echo 3 >/proc/sys/vm/drop_caches done for d in sda sdb; do umount /dev/\${d} done The stack trace is shown in below. [3310.967991] BTRFS: error (device sda) in btrfs_commit_transaction:2341: errno=-11 unknown (Error while writing out transaction) [3310.968060] BTRFS info (device sda): forced readonly [3310.968064] BTRFS warning (device sda): Skipping commit of aborted transaction. [3310.968065] ------------[cut here]------------ [3310.968066] BTRFS: Transaction aborted (error -11) [3310.968074] WARNING: CPU: 14 PID: 1684 at fs/btrfs/transaction.c:1946 btrfs_commit_transaction.cold+0x209/0x2c8 [3310.968131] CPU: 14 PID: 1684 Comm: fio Not tainted 5.14.10-300.fc35.x86_64 #1 [3310.968135] Hardware name: DIAWAY Tartu/Tartu, BIOS V2.01.B10 04/08/2021 [3310.968137] RIP: 0010:btrfs_commit_transaction.cold+0x209/0x2c8 [3310.968144] RSP: 0018:ffffb284ce393e10 EFLAGS: 00010282 [3310.968147] RAX: 0000000000000026 RBX: ffff973f147b0f60 RCX: 0000000000000027 [3310.968149] RDX: ffff974ecf098a08 RSI: 0000000000000001 RDI: ffff974ecf098a00 [3310.968150] RBP: ffff973f147b0f08 R08: 0000000000000000 R09: ffffb284ce393c48 [3310.968151] R10: ffffb284ce393c40 R11: ffffffff84f47468 R12: ffff973f101bfc00 [3310.968153] R13: ffff971f20cf2000 R14: 00000000ffffffff5 R15: ffff973f147b0e58 [3310.968154] FS: 00007efe65468740(0000) GS:ffff974ecf080000(0000) knlGS:0000000000000000 [3310.968157] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [3310.968158] CR2: 000055691bcbe260 CR3: 000000105cfa4001 CR4: 0000000000770ee0 [3310.968160] PKRU: 55555554 [3310.968161] Call Trace: [3310.968167] ? dput+0xd4/0x300 [3310.968174] btrfs_sync_file+0x3f1/0x490 [3310.968180] __x64_sys_fsync+0x33/0x60 [3310.968185] do_syscall_64+0x3b/0x90 [3310.968190] entry_SYSCALL_64_after_hwframe+0x44/0xae [3310.968194] RIP: 0033:0x7efe6557329b [3310.968200] RSP: 002b:00007ffe0236ebc0 EFLAGS: 00000293 ORIG_RAX: 000000000000004a [3310.968203] RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007efe6557329b [3310.968204] RDX: 0000000000000000 RSI: 00007efe58d77010 RDI: 0000000000000006 [3310.968205] RBP: 0000000004000000 R08: 0000000000000000 R09: 00007efe58d77010 [3310.968207] R10: 0000000016cacc0c R11: 0000000000000293 R12: 00007efe5ce95980 [3310.968208] R13: 0000000000000000 R14: 00007efe6447c790 R15: 0000000c80000000 [3310.968212] ---[end trace 1a346f4d3c0d96ba]--- [3310.968214] BTRFS: error (device sda) in cleanup_transaction:1946: errno=-11 unknown The abort occurs because of a write hole while writing out freeing tree nodes of a tree-log tree. For zoned btrfs, we re-dirty a freed tree node to ensure btrfs can write the region and does not leave a hole on write on a zoned device. The current code fails to re-dirty a node when the tree-log tree's depth is greater or equal to 2. That leads to a transaction abort with -EAGAIN. Fix the issue by properly re-dirtying a node on walking up the tree.	N/A	More Details
CVE-2021-47508	In the Linux kernel, the following vulnerability has been resolved: btrfs: free exchange changeset on failures Fstests runs on my VMs have show several kmemleak reports like the following. unreferenced object 0xffff88811ae59080 (size 64): comm "xfs_io", pid 12124, jiffies 4294987392 (age 6.368s) hex dump (first 32 bytes): 00 c0 1c 00 00 00 00 00 ff cf 1c 00 00 00 00 00 ..... 90 97 e5 1a 81 88 ff ff 90 97 e5 1a 81 88 ff ff ..... backtrace: [<00000000ac0176d2>] ulist_add_merge+0x60/0x150 [btrfs] [<0000000076e9f312>] set_state_bits+0x86/0xc0 [btrfs] [<0000000014fe73d6>] set_extent_bit+0x270/0x690 [btrfs] [<000000004f675208>] set_record_extent_bits+0x19/0x20 [btrfs] [<00000000b96137b1>] qgroup_reserve_data+0x274/0x310 [btrfs] [<0000000057e9dcbb>] btrfs_check_data_free_space+0x5c/0xa0 [btrfs] [<0000000019c4511d>] btrfs_delalloc_reserve_space+0x1b/0xa0 [btrfs] [<000000006d37e007>] btrfs_dio_iomap_begin+0x415/0x970 [btrfs] [<00000000fb8a74b8>] iomap_iter+0x161/0x1e0 [<0000000071dff6ff>] __iomap_dio_rw+0x1df/0x700 [<000000002567ba53>] iomap_dio_rw+0x5/0x20 [<0000000072e555f8>] btrfs_file_write_iter+0x290/0x530 [btrfs] [<000000005eb3d845>] new_sync_write+0x106/0x180 [<000000003fb505bf>] vfs_write+0x24d/0x2f0 [<000000009bb57d37>] __x64_sys_pwrite64+0x69/0xa0 [<000000003eba3fdf>] do_syscall_64+0x43/0x90 In case brtfs_qgroup_reserve_data() or btrfs_delalloc_reserve_metadata() fail the allocated extent_changeset will not be freed. So in btrfs_check_data_free_space() and btrfs_delalloc_reserve_space() free the allocated extent_changeset to get rid of the allocated memory. The issue currently only happens in the direct IO write path, but only after 65b3c08606e5 ("btrfs: fix ENOSPC failure when attempting direct IO write into NOCOW range"), and also at defrag_one_locked_target(). Every other place is always calling extent_changeset_free() even if its call to btrfs_delalloc_reserve_space() or btrfs_check_data_free_space() has failed.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47507	In the Linux kernel, the following vulnerability has been resolved: nfsd: Fix nsfd startup race (again) Commit bd5ae9288d64 ("nfsd: register pernet ops last, unregister first") has re-opened rpc_pipefs_event() race against nfsd_net_id registration (register_pernet_subsys()) which has been fixed by commit bb7ffbf29e76 ("nfsd: fix nsfd startup race triggering BUG_ON"). Restore the order of register_pernet_subsys() vs register_cld_notifier(). Add WARN_ON() to prevent a future regression. Crash info: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000012 CPU: 8 PID: 345 Comm: mount Not tainted 5.4.144-... #1 pc : rpc_pipefs_event+0x54/0x120 [nfsd] lr : rpc_pipefs_event+0x48/0x120 [nfsd] Call trace: rpc_pipefs_event+0x54/0x120 [nfsd] blocking_notifier_call_chain rpc_fill_super get_tree_keyed rpc_fs_get_tree vfs_get_tree do_mount ksys_mount __arm64_sys_mount el0_svc_handler el0_svc	N/A	More Details
CVE-2021-47506	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix use-after-free due to delegation race A delegation break could arrive as soon as we've called vfs_setlease. A delegation break runs a callback which immediately (in nfsd4_cb_recall_prepare) adds the delegation to del_recall_lru. If we then exit nfs4_set_delegation without hashing the delegation, it will be freed as soon as the callback is done with it, without ever being removed from del_recall_lru. Symptoms show up later as use-after-free or list corruption warnings, usually in the laundromat thread. I suspect aba2072f4523 "nfsd: grant read delegations to clients holding writes" made this bug easier to hit, but I looked as far back as v3.0 and it looks to me it already had the same problem. So I'm not sure where the bug was introduced; it may have been there from the beginning.	N/A	More Details
CVE-2021-47505	In the Linux kernel, the following vulnerability has been resolved: aio: fix use-after-free due to missing POLLFREE handling signalfd_poll() and binder_poll() are special in that they use a waitqueue whose lifetime is the current task, rather than the struct file as is normally the case. This is okay for blocking polls, since a blocking poll occurs within one task; however, non-blocking polls require another solution. This solution is for the queue to be cleared before it is freed, by sending a POLLFREE notification to all waiters. Unfortunately, only eventpoll handles POLLFREE. A second type of non-blocking poll, aio poll, was added in kernel v4.18, and it doesn't handle POLLFREE. This allows a use-after-free to occur if a signalfd or binder fd is polled with aio poll, and the waitqueue gets freed. Fix this by making aio poll handle POLLFREE. A patch by Ramji Jiyani <ramjiyani@google.com> (https://lore.kernel.org/r/20211027011834.2497484-1-ramjiyani@google.com) tried to do this by making aio_poll_wake() always complete the request inline if POLLFREE is seen. However, that solution had two bugs. First, it introduced a deadlock, as it unconditionally locked the aio context while holding the waitqueue lock, which inverts the normal locking order. Second, it didn't consider that POLLFREE notifications are missed while the request has been temporarily de-queued. The second problem was solved by my previous patch. This patch then properly fixes the use-after-free by handling POLLFREE in a deadlock-free way. It does this by taking advantage of the fact that freeing of the waitqueue is RCU-delayed, similar to what eventpoll does.	N/A	More Details
CVE-2021-47504	In the Linux kernel, the following vulnerability has been resolved: io_uring: ensure task_work gets run as part of cancelations If we successfully cancel a work item but that work item needs to be processed through task_work, then we can be sleeping uninterruptibly in io_uring_cancel_generic() and never process it. Hence we don't make forward progress and we end up with an uninterruptible sleep warning. While in there, correct a comment that should be IFF, not IIF.	N/A	More Details
CVE-2021-47501	In the Linux kernel, the following vulnerability has been resolved: i40e: Fix NULL pointer dereference in i40e_dbg_dump_desc When trying to dump VFs VSI RX/TX descriptors using debugfs there was a crash due to NULL pointer dereference in i40e_dbg_dump_desc. Added a check to i40e_dbg_dump_desc that checks if VSI type is correct for dumping RX/TX descriptors.	N/A	More Details
CVE-2021-47466	In the Linux kernel, the following vulnerability has been resolved: mm, slub: fix potential memoryleak in kmem_cache_open() In error path, the random_seq of slub cache might be leaked. Fix this by using __kmem_cache_release() to release all the relevant resources.	N/A	More Details
CVE-2021-47473	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix a memory leak in an error path of qla2x00_process_els() Commit 8c0eb596baa5 ("[SCSI] qla2xxx: Fix a memory leak in an error path of qla2x00_process_els()"), intended to change: bsg_job->request->msgcode == FC_BSG_HST_ELS_NOLOGIN bsg_job->request->msgcode != FC_BSG_RPT_ELS but changed it to: bsg_job->request->msgcode == FC_BSG_RPT_ELS instead. Change the == to a != to avoid leaking the fcport structure or freeing unallocated memory.	N/A	More Details
CVE-2021-47472	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-2021-47500	In the Linux kernel, the following vulnerability has been resolved: iio: mma8452: Fix trigger reference couting The mma8452 driver directly assigns a trigger to the struct iio_dev. The IIO core when done using this trigger will call `iio_trigger_put()` to drop the reference count by 1. Without the matching `iio_trigger_get()` in the driver the reference count can reach 0 too early, the trigger gets freed while still in use and a use-after-free occurs. Fix this by getting a reference to the trigger before assigning it to the IIO device.	N/A	More Details
CVE-2024-36011	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: HCI: Fix potential null-ptr-deref Fix potential null-ptr-deref in hci_le_big_sync_established_evt().	N/A	More Details
CVE-2021-47470	In the Linux kernel, the following vulnerability has been resolved: mm, slub: fix potential use-after-free in slab_debugfs_fops When sysfs_slab_add failed, we shouldn't call debugfs_slab_add() for s because s will be freed soon. And slab_debugfs_fops will use s later leading to a use-after-free.	N/A	More Details
CVE-2024-36012	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: msft: fix slab-use-after-free in msft_do_close() Tying the msft->data lifetime to hdev by freeing it in hci_release_dev() to fix the following case: [use] msft_do_close() msft = hdev->msft_data; if (!msft) ...(1) <- passed. return; mutex_lock(&msft->filter_lock); ...(4) <- used after freed. [free] msft_unregister() msft = hdev->msft_data; hdev->msft_data = NULL; ...(2) kfree(msft); ...(3) <- msft is freed. == BUG: KASAN: slab-use-after-free in __mutex_lock_common kernel/locking/mutex.c:587 [inline] BUG: KASAN: slab-use-after-free in __mutex_lock+0x8f/0xc30 kernel/locking/mutex.c:752 Read of size 8 at addr ffff888106cbbca8 by task kworker/u5:2/309	N/A	More Details
CVE-2021-47450	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix host stage-2 PGD refcount The KVM page-table library refcounts the pages of concatenated stage-2 PGDs individually. However, when running KVM in protected mode, the host's stage-2 PGD is currently managed by EL2 as a single high-order compound page, which can cause the refcount of the tail pages to reach 0 when they shouldn't, hence corrupting the page-table. Fix this by introducing a new hyp_split_page() helper in the EL2 page allocator (matching the kernel's split_page() function), and make use of it from host_s2_zalloc_pages_exact().	N/A	More Details
CVE-2021-47468	In the Linux kernel, the following vulnerability has been resolved: isdn: mISDN: Fix sleeping function called from invalid context The driver can call card->isac.release() function from an atomic context. Fix this by calling this function after releasing the lock. The following log reveals it: [44.168226] BUG: sleeping function called from invalid context at kernel/workqueue.c:3018 [44.168941] in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 5475, name: modprobe [44.169574] INFO: lockdep is turned off. [44.169899] irq event stamp: 0 [44.170160] hardirqs last enabled at (0): [<0000000000000000>] 0x0 [44.170627] hardirqs last disabled at (0): [<ffffffff814209ed>] copy_process+0x132d/0x3e00 [44.171240] softirqs last enabled at (0): [<ffffffff81420a1a>] copy_process+0x135a/0x3e00 [44.171852] softirqs last disabled at (0): [<0000000000000000>] 0x0 [44.172318] Preemption disabled at: [44.172320] [<ffffffffa009b0a9>] nj_release+0x69/0x500 [netjet] [44.174441] Call Trace: [44.174630] dump_stack_lvl+0xa8/0xd1 [44.174912] dump_stack+0x15/0x17 [44.175166] ___might_sleep+0x3a2/0x510 [44.175459] ? nj_release+0x69/0x500 [netjet] [44.175791] __might_sleep+0x82/0xe0 [44.176063] ? start_flush_work+0x20/0x7b0 [44.176375] start_flush_work+0x33/0x7b0 [44.176672] ? trace_irq_enable_rcuidle+0x85/0x170 [44.177034] ? kasan_quarantine_put+0xaa/0x1f0 [44.177372] ? kasan_quarantine_put+0xaa/0x1f0 [44.177711] __flush_work+0x11a/0x1a0 [44.177991] ? flush_work+0x20/0x20 [44.178257] ? lock_release+0x13c/0x8f0 [44.178550] ? __kasan_check_write+0x14/0x20 [44.178872] ? do_raw_spin_lock+0x148/0x360 [44.179187] ? read_lock_is_recursive+0x20/0x20 [44.179530] ? __kasan_check_read+0x11/0x20 [44.179846] ? do_raw_spin_unlock+0x55/0x900 [44.180168] ? ____kasan_slab_free+0x116/0x140 [44.180505] ? _raw_spin_unlock_irqrestore+0x41/0x60 [44.180878] ? skb_queue_purge+0x1a3/0x1c0 [44.181189] ? kfree+0x13e/0x290 [44.181438] flush_work+0x17/0x20 [44.181695] mISDN_freedchannel+0xe8/0x100 [44.182006] isac_release+0x210/0x260 [mISDNipac] [44.182366] nj_release+0xf6/0x500 [netjet] [44.182685] nj_remove+0x48/0x70 [netjet] [44.182989] pci_device_remove+0xa9/0x250	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47451	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_IDLETIMER: fix panic that occurs when timer_type has garbage value Currently, when the rule related to IDLETIMER is added, idletimer_tg timer structure is initialized by kmalloc on executing idletimer_tg_create function. However, in this process timer->timer_type is not defined to a specific value. Thus, timer->timer_type has garbage value and it occurs kernel panic. So, this commit fixes the panic by initializing timer->timer_type using kzalloc instead of kmalloc. Test commands: # iptables -A OUTPUT -j IDLETIMER --timeout 1 --label test $ cat /sys/class/xt_idletimer/timers/test Killed Splat looks like: BUG: KASAN: user-memory-access in alarm_expires_remaining+0x49/0x70 Read of size 8 at addr 0000002e8c7bc4c8 by task cat/917 CPU: 12 PID: 917 Comm: cat Not tainted 5.14.0+ #3 79940a339f71eb14fc81aee1757a20d5bf13eb0e Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.13.0-1ubuntu1.1 04/01/2014 Call Trace: dump_stack_lvl+0x6e/0x9c kasan_report.cold+0x112/0x117 ? alarm_expires_remaining+0x49/0x70 __asan_load8+0x86/0xb0 alarm_expires_remaining+0x49/0x70 idletimer_tg_show+0xe5/0x19b [xt_IDLETIMER 11219304af9316a21bee5ba9d58f76a6b9bccc6d] dev_attr_show+0x3c/0x60 sysfs_kf_seq_show+0x11d/0x1f0 ? device_remove_bin_file+0x20/0x20 kernfs_seq_show+0xa4/0xb0 seq_read_iter+0x29c/0x750 kernfs_fop_read_iter+0x25a/0x2c0 ? __fsnotify_parent+0x3d1/0x570 ? iov_iter_init+0x70/0x90 new_sync_read+0x2a7/0x3d0 ? __x64_sys_llseek+0x230/0x230 ? rw_verify_area+0x81/0x150 vfs_read+0x17b/0x240 ksys_read+0xd9/0x180 ? vfs_write+0x460/0x460 ? do_syscall_64+0x16/0xc0 ? lockdep_hardirqs_on+0x79/0x120 __x64_sys_read+0x43/0x50 do_syscall_64+0x3b/0xc0 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f0cdc819142 Code: c0 e9 c2 fe ff ff 50 48 8d 3d 3a ca 0a 00 e8 f5 19 02 00 0f 1f 44 00 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75 10 0f 05 <48> 3d 00 f0 ff ff 77 56 c3 0f 1f 44 00 00 48 83 ec 28 48 89 54 24 RSP: 002b:00007fff28eee5b8 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 RAX: ffffffffffffffda RBX: 0000000000020000 RCX: 00007f0cdc819142 RDX: 0000000000020000 RSI: 00007f0cdc032000 RDI: 0000000000000003 RBP: 00007f0cdc032000 R08: 00007f0cdc031010 R09: 0000000000000000 R10: 0000000000000022 R11: 0000000000000246 R12: 00005607e9ee31f0 R13: 0000000000000003 R14: 0000000000020000 R15: 0000000000020000	N/A	More Details
CVE-2021-47444	In the Linux kernel, the following vulnerability has been resolved: drm/edid: In connector_bad_edid() cap num_of_ext by num_blocks read In commit e11f5bd8228f ("drm: Add support for DP 1.4 Compliance edid corruption test") the function connector_bad_edid() started assuming that the memory for the EDID passed to it was big enough to hold `edid[0x7e] + 1` blocks of data (1 extra for the base block). It completely ignored the fact that the function was passed `num_blocks` which indicated how much memory had been allocated for the EDID. Let's fix this by adding a bounds check. This is important for handling the case where there's an error in the first block of the EDID. In that case we will call connector_bad_edid() without having re-allocated memory based on `edid[0x7e]`.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47448	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix possible stall on recvmsg() recvmsg() can enter an infinite loop if the caller provides the MSG_WAITALL, the data present in the receive queue is not sufficient to fulfill the request, and no more data is received by the peer. When the above happens, mptcp_wait_data() will always return with no wait, as the MPTCP_DATA_READY flag checked by such function is set and never cleared in such code path. Leveraging the above syzbot was able to trigger an RCU stall: rcu: INFO: rcu_preempt self-detected stall on CPU rcu: 0-...!: (10499 ticks this GP) idle=0af/1/0x4000000000000000 softirq=10678/10678 fqs=1 (t=10500 jiffies g=13089 q=109) rcu: rcu_preempt kthread starved for 10497 jiffies! g13089 f0x0 RCU_GP_WAIT_FQS(5) ->state=0x0 ->cpu=1 rcu: Unless rcu_preempt kthread gets sufficient CPU time, OOM is now expected behavior. rcu: RCU grace-period kthread stack dump: task:rcu_preempt state:R running task stack:28696 pid: 14 ppid: 2 flags:0x00004000 Call Trace: context_switch kernel/sched/core.c:4955 [inline] __schedule+0x940/0x26f0 kernel/sched/core.c:6236 schedule+0xd3/0x270 kernel/sched/core.c:6315 schedule_timeout+0x14a/0x2a0 kernel/time/timer.c:1881 rcu_gp_fqs_loop+0x186/0x810 kernel/rcu/tree.c:1955 rcu_gp_kthread+0x1de/0x320 kernel/rcu/tree.c:2128 kthread+0x405/0x4f0 kernel/kthread.c:327 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 rcu: Stack dump where RCU GP kthread last ran: Sending NMI from CPU 0 to CPUs 1: NMI backtrace for cpu 1 CPU: 1 PID: 8510 Comm: syz-executor827 Not tainted 5.15.0-rc2-next-20210920-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 RIP: 0010:bytes_is_nonzero mm/kasan/generic.c:84 [inline] RIP: 0010:memory_is_nonzero mm/kasan/generic.c:102 [inline] RIP: 0010:memory_is_poisoned_n mm/kasan/generic.c:128 [inline] RIP: 0010:memory_is_poisoned mm/kasan/generic.c:159 [inline] RIP: 0010:check_region_inline mm/kasan/generic.c:180 [inline] RIP: 0010:kasan_check_range+0xc8/0x180 mm/kasan/generic.c:189 Code: 38 00 74 ed 48 8d 50 08 eb 09 48 83 c0 01 48 39 d0 74 7a 80 38 00 74 f2 48 89 c2 b8 01 00 00 00 48 85 d2 75 56 5b 5d 41 5c c3 <48> 85 d2 74 5e 48 01 ea eb 09 48 83 c0 01 48 39 d0 74 50 80 38 00 RSP: 0018:ffffc9000cd676c8 EFLAGS: 00000283 RAX: ffffed100e9a110e RBX: ffffed100e9a110f RCX: ffffffff88ea062a RDX: 0000000000000001 RSI: 0000000000000008 RDI: ffff888074d08870 RBP: ffffed100e9a110e R08: 0000000000000001 R09: ffff888074d08877 R10: ffffed100e9a110e R11: 0000000000000000 R12: ffff888074d08000 R13: ffff888074d08000 R14: ffff888074d08088 R15: ffff888074d08000 FS: 0000555556d8e300(0000) GS:ffff8880b9d00000(0000) knlGS:0000000000000000 S: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000180 CR3: 0000000068909000 CR4: 00000000001506e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: instrument_atomic_read_write include/linux/instrumented.h:101 [inline] test_and_clear_bit include/asm-generic/bitops/instrumented-atomic.h:83 [inline] mptcp_release_cb+0x14a/0x210 net/mptcp/protocol.c:3016 release_sock+0xb4/0x1b0 net/core/sock.c:3204 mptcp_wait_data net/mptcp/protocol.c:1770 [inline] mptcp_recvmsg+0xfd1/0x27b0 net/mptcp/protocol.c:2080 inet6_recvmsg+0x11b/0x5e0 net/ipv6/af_inet6.c:659 sock_recvmsg_nosec net/socket.c:944 [inline] ____sys_recvmsg+0x527/0x600 net/socket.c:2626 ___sys_recvmsg+0x127/0x200 net/socket.c:2670 do_recvmmsg+0x24d/0x6d0 net/socket.c:2764 __sys_recvmmsg net/socket.c:2843 [inline] __do_sys_recvmmsg net/socket.c:2866 [inline] __se_sys_recvmmsg net/socket.c:2859 [inline] __x64_sys_recvmmsg+0x20b/0x260 net/socket.c:2859 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: 0033:0x7fc200d2 ---truncated---	N/A	More Details
CVE-2021-47433	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix abort logic in btrfs_replace_file_extents Error injection testing uncovered a case where we'd end up with a corrupt file system with a missing extent in the middle of a file. This occurs because the if statement to decide if we should abort is wrong. The only way we would abort in this case is if we got a ret != -EOPNOTSUPP and we called from the file clone code. However the prealloc code uses this path too. Instead we need to abort if there is an error, and the only error we _don't_ abort on is -EOPNOTSUPP and only if we came from the clone file code.	N/A	More Details
CVE-2024-5297	D-Link D-View executeWmicCmd Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the executeWmicCmd method. 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 root. Was ZDI-CAN-21821.	N/A	More Details
CVE-2024-5296	D-Link D-View Use of Hard-coded Cryptographic Key Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TokenUtils class. The issue results from a hard-coded cryptographic key. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-21991.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5295	D-Link G416 flupl self Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 wireless routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. 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 root. Was ZDI-CAN-21294.	N/A	More Details
CVE-2024-28060	An issue was discovered in Apiris Kafeo 6.4.4. It permits DLL hijacking, allowing a user to trigger the execution of arbitrary code every time the product is executed.	N/A	More Details
CVE-2024-31394	Directory traversal vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.12, Ver.3.0.x series versions prior to Ver.3.0.32, Ver.2.11.x series versions prior to Ver.2.11.61, Ver.2.10.x series versions prior to Ver.2.10.53, and Ver.2.9 and earlier versions. If this vulnerability is exploited, a user with an editor or higher privilege who can log in to the product may obtain arbitrary files on the server.	N/A	More Details
CVE-2024-5294	D-Link DIR-3040 prog.cgi websSecurityHandler Memory Leak Denial-of-Service Vulnerability. This vulnerability allows network-adjacent attackers to create a denial-of-service condition on affected installations of D-Link DIR-3040 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prog.cgi program, which handles HNAP requests made to the lighttpd webserver listening on ports 80 and 443. The issue results from the lack of proper memory management when processing HTTP cookie values. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. . Was ZDI-CAN-21668.	N/A	More Details
CVE-2024-5293	D-Link DIR-2640 HTTP Referer Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640-US routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within prog.cgi, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. 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 root. Was ZDI-CAN-21853.	N/A	More Details
CVE-2024-5292	D-Link Network Assistant Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of D-Link Network Assistant. 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 DNACore service. The service loads 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-21426.	N/A	More Details
CVE-2024-5291	D-Link DIR-2150 GetDeviceSettings Target Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. 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 root. Was ZDI-CAN-21235.	N/A	More Details
CVE-2024-5247	NETGEAR ProSAFE Network Management System UpLoadServlet Unrestricted File Upload 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 UpLoadServlet class. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22923.	N/A	More Details
CVE-2024-5245	NETGEAR ProSAFE Network Management System Default Credentials Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. 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 product installer. The issue results from the use of default MySQL credentials. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-22755.	N/A	More Details
CVE-2024-5244	TP-Link Omada ER605 Reliance on Security Through Obscurity Vulnerability. This vulnerability allows network-adjacent attackers to access or spoof DDNS messages on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the cmxddnsd executable. The issue results from reliance on obscurity to secure network data. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-22439.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5243	TP-Link Omada ER605 Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the handling of DNS names. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22523.	N/A	More Details
CVE-2024-5242	TP-Link Omada ER605 Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the handling of DDNS error codes. 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 root. Was ZDI-CAN-22522.	N/A	More Details
CVE-2024-5228	TP-Link Omada ER605 Comexe DDNS Response Handling Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the handling of DNS responses. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22383.	N/A	More Details
CVE-2024-5227	TP-Link Omada ER605 PPTP VPN username Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are only vulnerable if configured to use a PPTP VPN with LDAP authentication. The specific flaw exists within the handling of the username parameter provided to the /usr/bin/pppd endpoint. 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 root. Was ZDI-CAN-22446.	N/A	More Details
CVE-2024-5190	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-2023-30309	An issue discovered in D-Link DI-7003GV2 routers allows attackers to hijack TCP sessions which could lead to a denial of service.	N/A	More Details
CVE-2023-30307	An issue discovered in TP-LINK TL-R473GP-AC, TP-LINK XDR6020, TP-LINK TL-R479GP-AC, TP-LINK TL-R4239G, TP-LINK TL-WAR1200L, and TP-LINK TL-R476G routers allows attackers to hijack TCP sessions which could lead to a denial of service.	N/A	More Details
CVE-2021-47447	In the Linux kernel, the following vulnerability has been resolved: drm/msm/a3xx: fix error handling in a3xx_gpu_init() These error paths returned 1 on failure, instead of a negative error code. This would lead to an Oops in the caller. A second problem is that the check for "if (ret != -ENODATA)" did not work because "ret" was set to 1.	N/A	More Details
CVE-2024-5298	D-Link D-View queryDeviceCustomMonitorResult Exposed Dangerous Method Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the queryDeviceCustomMonitorResult method. The issue results from an exposed dangerous method. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21842.	N/A	More Details
CVE-2024-5142	Stored Cross-Site Scripting vulnerability in Social Module in M-Files Hubshare before version 5.0.6.0 allows authenticated attacker to run scripts in other users browser	N/A	More Details
CVE-2021-47446	In the Linux kernel, the following vulnerability has been resolved: drm/msm/a4xx: fix error handling in a4xx_gpu_init() This code returns 1 on error instead of a negative error. It leads to an Oops in the caller. A second problem is that the check for "if (ret != -ENODATA)" cannot be true because "ret" is set to 1.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47445	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix null pointer dereference on pointer edp The initialization of pointer dev dereferences pointer edp before edp is null checked, so there is a potential null pointer deference issue. Fix this by only dereferencing edp after edp has been null checked. Addresses-Coverity: ("Dereference before null check")	N/A	More Details
CVE-2021-47474	In the Linux kernel, the following vulnerability has been resolved: comedi: vmk80xx: fix bulk-buffer overflow The driver is using endpoint-sized buffers but must not assume that the tx and rx buffers are of equal size or a malicious device could overflow the slab-allocated receive buffer when doing bulk transfers.	N/A	More Details
CVE-2021-47442	In the Linux kernel, the following vulnerability has been resolved: NFC: digital: fix possible memory leak in digital_in_send_sdd_req() 'skb' is allocated in digital_in_send_sdd_req(), but not free when digital_in_send_cmd() failed, which will cause memory leak. Fix it by freeing 'skb' if digital_in_send_cmd() return failed.	N/A	More Details
CVE-2023-4859	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-27957. Reason: This candidate is a duplicate of CVE-2024-27957. Notes: All CVE users should reference CVE-2024-27957 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-2301	Certain HP LaserJet Pro devices are potentially vulnerable to a Cross-Site Scripting (XSS) attack via the web management interface of the device.	N/A	More Details
CVE-2021-47438	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix memory leak in mlx5_core_destroy_cq() error path Prior to this patch in case mlx5_core_destroy_cq() failed it returns without completing all destroy operations and that leads to memory leak. Instead, complete the destroy flow before return error. Also move mlx5_debug_cq_remove() to the beginning of mlx5_core_destroy_cq() to be symmetrical with mlx5_core_create_cq(). kmemleak complains on: unreferenced object 0xc000000038625100 (size 64): comm "ethtool", pid 28301, jiffies 4298062946 (age 785.380s) hex dump (first 32 bytes): 60 01 48 94 00 00 00 c0 b8 05 34 c3 00 00 00 c0 `.H.....4..... 02 00 00 00 00 00 00 00 00 db 7d c1 00 00 00 c0 ....}..... backtrace: [<000000009e8643cb>] add_res_tree+0xd0/0x270 [mlx5_core] [<00000000e7cb8e6c>] mlx5_debug_cq_add+0x5c/0xc0 [mlx5_core] [<000000002a12918f>] mlx5_core_create_cq+0x1d0/0x2d0 [mlx5_core] [<00000000cef0a696>] mlx5e_create_cq+0x210/0x3f0 [mlx5_core] [<000000009c642c26>] mlx5e_open_cq+0xb4/0x130 [mlx5_core] [<0000000058dfa578>] mlx5e_ptp_open+0x7f4/0xe10 [mlx5_core] [<0000000081839561>] mlx5e_open_channels+0x9cc/0x13e0 [mlx5_core] [<0000000009cf05d4>] mlx5e_switch_priv_channels+0xa4/0x230 [mlx5_core] [<0000000042bbedd8>] mlx5e_safe_switch_params+0x14c/0x300 [mlx5_core] [<0000000004bc9db8>] set_pflag_tx_port_ts+0x9c/0x160 [mlx5_core] [<00000000a0553443>] mlx5e_set_priv_flags+0xd0/0x1b0 [mlx5_core] [<00000000a8f3d84b>] ethnl_set_privflags+0x234/0x2d0 [<00000000fd27f27c>] genl_family_rcv_msg_doit+0x108/0x1d0 [<00000000f495e2bb>] genl_family_rcv_msg+0xe4/0x1f0 [<00000000646c5c2c>] genl_rcv_msg+0x78/0x120 [<00000000d53e384e>] netlink_rcv_skb+0x74/0x1a0	N/A	More Details
CVE-2023-43850	Improper input validation in the user management function of web interface in Aten PE6208 2.3.228 and 2.4.232 allows remote authenticated users to cause a partial DoS of web interface via HTTP POST request.	N/A	More Details
CVE-2021-47437	In the Linux kernel, the following vulnerability has been resolved: iio: adis16475: fix deadlock on frequency set With commit 39c024b51b560 ("iio: adis16475: improve sync scale mode handling"), two deadlocks were introduced: 1) The call to 'adis_write_reg_16()' was not changed to it's unlocked version. 2) The lock was not being released on the success path of the function. This change fixes both these issues.	N/A	More Details
CVE-2024-33450	SQL Injection in Finereport v.8.0 allows a remote attacker to obtain sensitive information	N/A	More Details
CVE-2024-5299	D-Link D-View execMonitorScript Exposed Dangerous Method Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the execMonitorScript method. The issue results from an exposed dangerous method. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21828.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47436	In the Linux kernel, the following vulnerability has been resolved: usb: musb: dsps: Fix the probe error path Commit 7c75bde329d7 ("usb: musb: musb_dsps: request_irq() after initializing musb") has inverted the calls to dsps_setup_optional_vbus_irq() and dsps_create_musb_pdev() without updating correctly the error path. dsps_create_musb_pdev() allocates and registers a new platform device which must be unregistered and freed with platform_device_unregister(), and this is missing upon dsps_setup_optional_vbus_irq() error. While on the master branch it seems not to trigger any issue, I observed a kernel crash because of a NULL pointer dereference with a v5.10.70 stable kernel where the patch mentioned above was backported. With this kernel version, -EPROBE_DEFER is returned the first time dsps_setup_optional_vbus_irq() is called which triggers the probe to error out without unregistering the platform device. Unfortunately, on the Beagle Bone Black Wireless, the platform device still living in the system is being used by the USB Ethernet gadget driver, which during the boot phase triggers the crash. My limited knowledge of the musb world prevents me to revert this commit which was sent to silence a robot warning which, as far as I understand, does not make sense. The goal of this patch was to prevent an IRQ to fire before the platform device being registered. I think this cannot ever happen due to the fact that enabling the interrupts is done by the ->enable() callback of the platform musb device, and this platform device must be already registered in order for the core or any other user to use this callback. Hence, I decided to fix the error path, which might prevent future errors on mainline kernels while also fixing older ones.	N/A	More Details
CVE-2021-47435	In the Linux kernel, the following vulnerability has been resolved: dm: fix mempool NULL pointer race when completing IO dm_io_dec_pending() calls end_io_acct() first and will then dec md in-flight pending count. But if a task is swapping DM table at same time this can result in a crash due to mempool->elements being NULL: task1 task2 do_resume ->do_suspend ->dm_wait_for_completion bio_endio ->clone_endio ->dm_io_dec_pending ->end_io_acct ->wakeup task1 ->dm_swap_table ->__bind ->__bind_mempools ->bioset_exit ->mempool_exit ->free_io [67.330330] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 ..... [67.330494] pstate: 80400085 (Nzcv daIf +PAN -UAO) [67.330510] pc : mempool_free+0x70/0xa0 [67.330515] lr : mempool_free+0x4c/0xa0 [67.330520] sp : ffffff8008013b20 [67.330524] x29: ffffff8008013b20 x28: 0000000000000004 [67.330530] x27: ffffffa8c2ff40a0 x26: 00000000ffff1cc8 [67.330535] x25: 0000000000000000 x24: ffffffdada34c800 [67.330541] x23: 0000000000000000 x22: ffffffdada34c800 [67.330547] x21: 00000000ffff1cc8 x20: ffffffd9a1304d80 [67.330552] x19: ffffffdada34c970 x18: 000000b312625d9c [67.330558] x17: 00000000002dcfbf x16: 00000000000006dd [67.330563] x15: 000000000093b41e x14: 0000000000000010 [67.330569] x13: 0000000000007f7a x12: 0000000034155555 [67.330574] x11: 0000000000000001 x10: 0000000000000001 [67.330579] x9 : 0000000000000000 x8 : 0000000000000000 [67.330585] x7 : 0000000000000000 x6 : ffffff80148b5c1a [67.330590] x5 : ffffff8008013ae0 x4 : 0000000000000001 [67.330596] x3 : ffffff80080139c8 x2 : ffffff801083bab8 [67.330601] x1 : 0000000000000000 x0 : ffffffdada34c970 [67.330609] Call trace: [67.330616] mempool_free+0x70/0xa0 [67.330627] bio_put+0xf8/0x110 [67.330638] dec_pending+0x13c/0x230 [67.330644] clone_endio+0x90/0x180 [67.330649] bio_endio+0x198/0x1b8 [67.330655] dec_pending+0x190/0x230 [67.330660] clone_endio+0x90/0x180 [67.330665] bio_endio+0x198/0x1b8 [67.330673] blk_update_request+0x214/0x428 [67.330683] scsi_end_request+0x2c/0x300 [67.330688] scsi_io_completion+0xa0/0x710 [67.330695] scsi_finish_command+0xd8/0x110 [67.330700] scsi_softirq_done+0x114/0x148 [67.330708] blk_done_softirq+0x74/0xd0 [67.330716] __do_softirq+0x18c/0x374 [67.330724] irq_exit+0xb4/0xb8 [67.330732] __handle_domain_irq+0x84/0xc0 [67.330737] gic_handle_irq+0x148/0x1b0 [67.330744] el1_irq+0xe8/0x190 [67.330753] lpm_cpuidle_enter+0x4f8/0x538 [67.330759] cpuidle_enter_state+0x1fc/0x398 [67.330764] cpuidle_enter+0x18/0x20 [67.330772] do_idle+0x1b4/0x290 [67.330778] cpu_startup_entry+0x20/0x28 [67.330786] secondary_start_kernel+0x160/0x170 Fix this by: 1) Establishing pointers to 'struct dm_io' members in dm_io_dec_pending() so that they may be passed into end_io_acct() _after_ free_io() is called. 2) Moving end_io_acct() after free_io().	N/A	More Details
CVE-2024-5433	The Campbell Scientific CSI Web Server supports a command that will return the most recent file that matches a given expression. A specially crafted expression can lead to a path traversal vulnerability. This command combined with a specially crafted expression allows anonymous, unauthenticated access (allowed by default) by an attacker to files and directories outside of the webserver root directory they should be restricted to.	N/A	More Details
CVE-2024-5434	The Campbell Scientific CSI Web Server stores web authentication credentials in a file with a specific file name. Passwords within that file are stored in a weakly encoded format. There is no known way to remotely access the file unless it has been manually renamed. However, if an attacker were to gain access to the file, passwords could be decoded and reused to gain access.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47434	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix command ring pointer corruption while aborting a command The command ring pointer is located at [6:63] bits of the command ring control register (CRCR). All the control bits like command stop, abort are located at [0:3] bits. While aborting a command, we read the CRCR and set the abort bit and write to the CRCR. The read will always give command ring pointer as all zeros. So we essentially write only the control bits. Since we split the 64 bit write into two 32 bit writes, there is a possibility of xHC command ring stopped before the upper dword (all zeros) is written. If that happens, xHC updates the upper dword of its internal command ring pointer with all zeros. Next time, when the command ring is restarted, we see xHC memory access failures. Fix this issue by only writing to the lower dword of CRCR where all control bits are located.	N/A	More Details
CVE-2021-47515	In the Linux kernel, the following vulnerability has been resolved: seg6: fix the iif in the IPv6 socket control block When an IPv4 packet is received, the ip_rcv_core(...) sets the receiving interface index into the IPv4 socket control block (v5.16-rc4, net/ipv4/ip_input.c line 510): IPCB(skb)->iif = skb->skb_iif; If that IPv4 packet is meant to be encapsulated in an outer IPv6+SRH header, the seg6_do_srh_encap(...) performs the required encapsulation. In this case, the seg6_do_srh_encap function clears the IPv6 socket control block (v5.16-rc4 net/ipv6/seg6_iptunnel.c line 163): memset(IP6CB(skb), 0, sizeof(*IP6CB(skb))); The memset(...) was introduced in commit ef489749aae5 ("ipv6: sr: clear IP6CB(skb) on SRH ip4ip6 encapsulation") a long time ago (2019-01-29). Since the IPv6 socket control block and the IPv4 socket control block share the same memory area (skb->cb), the receiving interface index info is lost (IP6CB(skb)->iif is set to zero). As a side effect, that condition triggers a NULL pointer dereference if commit 0857d6f8c759 ("ipv6: When forwarding count rx stats on the orig netdev") is applied. To fix that issue, we set the IP6CB(skb)->iif with the index of the receiving interface once again.	N/A	More Details
CVE-2021-47480	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Put LLD module refcnt after SCSI device is released SCSI host release is triggered when SCSI device is freed. We have to make sure that the low-level device driver module won't be unloaded before SCSI host instance is released because shost->hostt is required in the release handler. Make sure to put LLD module refcnt after SCSI device is released. Fixes a kernel panic of 'BUG: unable to handle page fault for address' reported by Changhui and Yi.	N/A	More Details
CVE-2021-47475	In the Linux kernel, the following vulnerability has been resolved: comedi: vmk80xx: fix transfer-buffer overflows The driver uses endpoint-sized USB transfer buffers but up until recently had no sanity checks on the sizes. Commit e1f13c879a7c ("staging: comedi: check validity of wMaxPacketSize of usb endpoints found") inadvertently fixed NULL-pointer dereferences when accessing the transfer buffers in case a malicious device has a zero wMaxPacketSize. Make sure to allocate buffers large enough to handle also the other accesses that are done without a size check (e.g. byte 18 in vmk80xx_cnt_insn_read() for the VMK8061_MODEL) to avoid writing beyond the buffers, for example, when doing descriptor fuzzing. The original driver was for a low-speed device with 8-byte buffers. Support was later added for a device that uses bulk transfers and is presumably a full-speed device with a maximum 64-byte wMaxPacketSize.	N/A	More Details
CVE-2024-4535	The KKProgressbar2 Free WordPress plugin through 1.1.4.2 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	N/A	More Details
CVE-2024-3594	The IDonate WordPress plugin through 1.9.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	More Details
CVE-2024-3939	The Ditty WordPress plugin before 3.1.36 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	More Details
CVE-2021-47569	In the Linux kernel, the following vulnerability has been resolved: io_uring: fail cancellation for EXITING tasks WARNING: CPU: 1 PID: 20 at fs/io_uring.c:6269 io_try_cancel_userdata+0x3c5/0x640 fs/io_uring.c:6269 CPU: 1 PID: 20 Comm: kworker/1:0 Not tainted 5.16.0-rc1-syzkaller #0 Workqueue: events io_fallback_req_func RIP: 0010:io_try_cancel_userdata+0x3c5/0x640 fs/io_uring.c:6269 Call Trace: <TASK> io_req_task_link_timeout+0x6b/0x1e0 fs/io_uring.c:6886 io_fallback_req_func+0xf9/0x1ae fs/io_uring.c:1334 process_one_work+0x9b2/0x1690 kernel/workqueue.c:2298 worker_thread+0x658/0x11f0 kernel/workqueue.c:2445 kthread+0x405/0x4f0 kernel/kthread.c:327 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK> We need original task's context to do cancellations, so if it's dying and the callback is executed in a fallback mode, fail the cancellation attempt.	N/A	More Details
CVE-2021-47568	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix memleak in get_file_stream_info() Fix memleak in get_file_stream_info()	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47567	In the Linux kernel, the following vulnerability has been resolved: powerpc/32: Fix hardlockup on vmap stack overflow Since the commit c118c7303ad5 ("powerpc/32: Fix vmap stack - Do not activate MMU before reading task struct") a vmap stack overflow results in a hard lockup. This is because emergency_ctx is still addressed with its virtual address allthough data MMU is not active anymore at that time. Fix it by using a physical address instead.	N/A	More Details
CVE-2024-35554	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoWeb_deal.php?mudi=del&dataType=newsWeb&dataTypeCN.	N/A	More Details
CVE-2024-4533	The KKProgressbar2 Free WordPress plugin through 1.1.4.2 does not sanitize and escape a parameter before using it in a SQL statement, allowing admin users to perform SQL injection attacks	N/A	More Details
CVE-2021-47566	In the Linux kernel, the following vulnerability has been resolved: proc/vmcore: fix clearing user buffer by properly using clear_user() To clear a user buffer we cannot simply use memset, we have to use clear_user(). With a virtio-mem device that registers a vmcore_cb and has some logically unplugged memory inside an added Linux memory block, I can easily trigger a BUG by copying the vmcore via "cp": systemd[1]: Starting Kdump Vmcore Save Service... kdump[420]: Kdump is using the default log level(3). kdump[453]: saving to /sysroot/var/crash/127.0.0.1-2021-11-11-14:59:22/ kdump[458]: saving vmcore-dmesg.txt to /sysroot/var/crash/127.0.0.1-2021-11-11-14:59:22/ kdump[465]: saving vmcore-dmesg.txt complete kdump[467]: saving vmcore BUG: unable to handle page fault for address: 00007f2374e01000 #PF: supervisor write access in kernel mode #PF: error_code(0x0003) - permissions violation PGD 7a523067 P4D 7a523067 PUD 7a528067 PMD 7a525067 PTE 800000007048f867 Oops: 0003 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 468 Comm: cp Not tainted 5.15.0+ #6 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.14.0-27-g64f37cc530f1-prebuilt.qemu.org 04/01/2014 RIP: 0010:read_from_oldmem.part.0.cold+0x1d/0x86 Code: ff ff ff e8 05 ff fe ff e9 b9 e9 7f ff 48 89 de 48 c7 c7 38 3b 60 82 e8 f1 fe fe ff 83 fd 08 72 3c 49 8d 7d 08 4c 89 e9 89 e8 <49> c7 45 00 00 00 00 00 49 c7 44 05 f8 00 00 00 00 48 83 e7 f81 RSP: 0018:ffffc9000073be08 EFLAGS: 00010212 RAX: 0000000000001000 RBX: 00000000002fd000 RCX: 00007f2374e01000 RDX: 0000000000000001 RSI: 00000000ffffdfff RDI: 00007f2374e01008 RBP: 0000000000001000 R08: 0000000000000000 R09: ffffc9000073bc50 R10: ffffc9000073bc48 R11: ffffffff829461a8 R12: 000000000000f000 R13: 00007f2374e01000 R14: 0000000000000000 R15: ffff88807bd421e8 FS: 00007f2374e12140(0000) GS:ffff88807f000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f2374e01000 CR3: 000000007a4aa000 CR4: 0000000000350eb0 Call Trace: read_vmcore+0x236/0x2c0 proc_reg_read+0x55/0xa0 vfs_read+0x95/0x190 ksys_read+0x4f/0xc0 do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae Some x86-64 CPUs have a CPU feature called "Supervisor Mode Access Prevention (SMAP)", which is used to detect wrong access from the kernel to user buffers like this: SMAP triggers a permissions violation on wrong access. In the x86-64 variant of clear_user(), SMAP is properly handled via clac()+stac(). To fix, properly use clear_user() when we're dealing with a user buffer.	N/A	More Details
CVE-2024-35551	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoWeb_deal.php?mudi=add.	N/A	More Details
CVE-2023-50977	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability. See also CVE-2024-36472.	N/A	More Details
CVE-2024-35550	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoWeb_deal.php?mudi=rev.	N/A	More Details
CVE-2024-5035	The affected device expose a network service called "rftest" that is vulnerable to unauthenticated command injection on ports TCP/8888, TCP/8889, and TCP/8890. By successfully exploiting this flaw, remote unauthenticated attacker can gain arbitrary command execution on the device with elevated privileges.This issue affects Archer C4500X: through 1_1.1.6.	N/A	More Details
CVE-2021-47565	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Fix kernel panic during drive powercycle test While looping over shost's sdev list it is possible that one of the drives is getting removed and its sas_target object is freed but its sdev object remains intact. Consequently, a kernel panic can occur while the driver is trying to access the sas_address field of sas_target object without also checking the sas_target object for NULL.	N/A	More Details
CVE-2023-6349	A heap overflow vulnerability exists in libvpx - Encoding a frame that has larger dimensions than the originally configured size with VP9 may result in a heap overflow in libvpx. We recommend upgrading to version 1.13.1 or above	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47564	In the Linux kernel, the following vulnerability has been resolved: net: marvell: prestera: fix double free issue on err path fix error path handling in prestera_bridge_port_join() that cases prestera driver to crash (see below). Trace: Internal error: Oops: 96000044 [#1] SMP Modules linked in: prestera_pci prestera uio_pdrv_genirq CPU: 1 PID: 881 Comm: ip Not tainted 5.15.0 #1 pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : prestera_bridge_destroy+0x2c/0xb0 [prestera] lr : prestera_bridge_port_join+0x2cc/0x350 [prestera] sp : ffff800011a1b0f0 ... x2 : ffff000109ca6c80 x1 : dead000000000100 x0 : dead000000000122 Call trace: prestera_bridge_destroy+0x2c/0xb0 [prestera] prestera_bridge_port_join+0x2cc/0x350 [prestera] prestera_netdev_port_event.constprop.0+0x3c4/0x450 [prestera] prestera_netdev_event_handler+0xf4/0x110 [prestera] raw_notifier_call_chain+0x54/0x80 call_netdevice_notifiers_info+0x54/0xa0 __netdev_upper_dev_link+0x19c/0x380	N/A	More Details
CVE-2021-47562	In the Linux kernel, the following vulnerability has been resolved: ice: fix vsi->txq_map sizing The approach of having XDP queue per CPU regardless of user's setting exposed a hidden bug that could occur in case when Rx queue count differ from Tx queue count. Currently vsi->txq_map's size is equal to the doubled vsi->alloc_txq, which is not correct due to the fact that XDP rings were previously based on the Rx queue count. Below splat can be seen when ethtool -L is used and XDP rings are configured: [682.875339] BUG: kernel NULL pointer dereference, address: 000000000000000f [682.883403] #PF: supervisor read access in kernel mode [682.889345] #PF: error_code(0x0000) - not-present page [682.895289] PGD 0 P4D 0 [682.898218] Oops: 0000 [#1] PREEMPT SMP PTI [682.903055] CPU: 42 PID: 2878 Comm: ethtool Tainted: G OE 5.15.0-rc5+ #1 [682.912214] Hardware name: Intel Corp. GRANTLEY/GRANTLEY, BIOS GRRFCRB1.86B.0276.D07.1605190235 05/19/2016 [682.923380] RIP: 0010:devres_remove+0x44/0x130 [682.928527] Code: 49 89 f4 55 48 89 fd 4c 89 ff 53 48 83 ec 10 e8 92 b9 49 00 48 8b 9d a8 02 00 00 48 8d 8d a0 02 00 00 49 89 c2 48 39 cb 74 0f <4c> 3b 63 10 74 25 48 8b 5b 08 48 39 cb 75 f1 4c 89 ff 4c 89 d6 e8 [682.950237] RSP: 0018:ffffc90006a679f0 EFLAGS: 00010002 [682.956285] RAX: 0000000000000286 RBX: ffffffffffffffff RCX: ffff88908343a370 [682.964538] RDX: 0000000000000001 RSI: ffffffff81690d60 RDI: 0000000000000000 [682.972789] RBP: ffff88908343a0d0 R08: 0000000000000000 R09: 0000000000000000 [682.981040] R10: 0000000000000286 R11: 3fffffffffffffff R12: ffffffff81690d60 [682.989282] R13: ffffffff81690a00 R14: ffff8890819807a8 R15: ffff88908343a36c [682.997535] FS: 00007f08c7bfa740(0000) GS:ffff88a03fd00000(0000) knlGS:0000000000000000 [683.006910] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [683.013557] CR2: 000000000000000f CR3: 0000001080a66003 CR4: 00000000003706e0 [683.021819] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [683.030075] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [683.038336] Call Trace: [683.041167] devm_kfree+0x33/0x50 [683.045004] ice_vsi_free_arrays+0x5e/0xc0 [ice] [683.050380] ice_vsi_rebuild+0x4c8/0x750 [ice] [683.055543] ice_vsi_recfg_qs+0x9a/0x110 [ice] [683.060697] ice_set_channels+0x14f/0x290 [ice] [683.065962] ethnl_set_channels+0x333/0x3f0 [683.070807] genl_family_rcv_msg_doit+0xea/0x150 [683.076152] genl_rcv_msg+0xde/0x1d0 [683.080289] ? channels_prepare_data+0x60/0x60 [683.085432] ? genl_get_cmd+0xd0/0xd0 [683.089667] netlink_rcv_skb+0x50/0xf0 [683.094006] genl_rcv+0x24/0x40 [683.097638] netlink_unicast+0x239/0x340 [683.102177] netlink_sendmsg+0x22e/0x470 [683.106717] sock_sendmsg+0x5e/0x60 [683.110756] __sys_sendto+0xee/0x150 [683.114894] ? handle_mm_fault+0xd0/0x2a0 [683.119535] ? do_user_addr_fault+0x1f3/0x690 [683.134173] __x64_sys_sendto+0x25/0x30 [683.148231] do_syscall_64+0x3b/0xc0 [683.161992] entry_SYSCALL_64_after_hwframe+0x44/0xae Fix this by taking into account the value that num_possible_cpus() yields in addition to vsi->alloc_txq instead of doubling the latter.	N/A	More Details
CVE-2024-3381	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-36010	In the Linux kernel, the following vulnerability has been resolved: igb: Fix string truncation warnings in igb_set_fw_version Commit 1978d3ead82c ("intel: fix string truncation warnings") fixes '-Wformat-truncation=' warnings in igb_main.c by using kasprintf. drivers/net/ethernet/intel/igb/igb_main.c:3092:53: warning：‘%d’ directive output may be truncated writing between 1 and 5 bytes into a region of size between 1 and 13 [-Wformat-truncation=] 3092 | "%d.%d, 0x%08x, %d.%d.%d", | ^~ drivers/net/ethernet/intel/igb/igb_main.c:3092:34: note：directive argument in the range [0, 65535] 3092 | "%d.%d, 0x%08x, %d.%d.%d", | ^~~~~~~~~~~~~~~~~~~~~~~~~~ drivers/net/ethernet/intel/igb/igb_main.c:3092:34: note：directive argument in the range [0, 65535] drivers/net/ethernet/intel/igb/igb_main.c:3090:25: note：‘snprintf’ output between 23 and 43 bytes into a destination of size 32 kasprintf() returns a pointer to dynamically allocated memory which can be NULL upon failure. Fix this warning by using a larger space for adapter->fw_version, and then fall back and continue to use snprintf.	N/A	More Details
CVE-2024-33809	PingCAP TiDB v7.5.1 was discovered to contain a buffer overflow vulnerability, which could lead to database crashes and denial of service attacks.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35560	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/ca_deal.php?mudi=del&dataType=&dataTypeCN.	N/A	More Details
CVE-2023-52880	In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: require CAP_NET_ADMIN to attach N_GSM0710 ldisc Any unprivileged user can attach N_GSM0710 ldisc, but it requires CAP_NET_ADMIN to create a GSM network anyway. Require initial namespace CAP_NET_ADMIN to do that.	N/A	More Details
CVE-2024-33427	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-2023-51636	Avira Prime Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Avira Prime. 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 Avira Spotlight Service. By creating a symbolic link, an attacker can abuse the service 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-21600.	N/A	More Details
CVE-2023-51637	Sante PACS Server PG Patient Query SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante PACS Server PG. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the DICOM service, which listens on TCP port 11122 by default. When parsing the NAME element of the PATIENT record, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE. Was ZDI-CAN-21579.	N/A	More Details
CVE-2024-4267	A remote code execution (RCE) vulnerability exists in the parisneo/lollms-webui, specifically within the 'open_file' module, version 9.5. The vulnerability arises due to improper neutralization of special elements used in a command within the 'open_file' function. An attacker can exploit this vulnerability by crafting a malicious file path that, when processed by the 'open_file' function, executes arbitrary system commands or reads sensitive file content. This issue is present in the code where subprocess.Popen is used unsafely to open files based on user-supplied paths without adequate validation, leading to potential command injection.	N/A	More Details
CVE-2024-4286	Mintplex-Labs' anything-llm application is vulnerable to improper neutralization of special elements used in an expression language statement, identified in the commit id `57984fa85c31988b2eff429adfc654c46e0c342a`. The vulnerability arises from the application's handling of user modifications by managers or admins, allowing for the modification of all existing attributes of the `user` database entity without proper checks or sanitization. This flaw can be exploited to delete user threads, denying users access to their previously submitted data, or to inject fake threads and/or chat history for social engineering attacks.	N/A	More Details
CVE-2024-4454	WithSecure Elements Endpoint Protection Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of WithSecure Elements Endpoint Protection. User interaction on the part of an administrator is required to exploit this vulnerability. The specific flaw exists within the WithSecure plugin hosting service. By creating a symbolic link, an attacker can abuse the service to create a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23035.	N/A	More Details
CVE-2023-46806	An SQL Injection vulnerability in a web component of EPMM versions before 12.1.0.0 allows an authenticated user with appropriate privilege to access or modify data in the underlying database.	N/A	More Details
CVE-2023-46807	An SQL Injection vulnerability in web component of EPMM before 12.1.0.0 allows an authenticated user with appropriate privilege to access or modify data in the underlying database.	N/A	More Details
CVE-2024-30657	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-30658	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29849	Veeam Backup Enterprise Manager allows unauthenticated users to log in as any user to enterprise manager web interface.	N/A	More Details
CVE-2024-29850	Veeam Backup Enterprise Manager allows account takeover via NTLM relay.	N/A	More Details
CVE-2024-29851	Veeam Backup Enterprise Manager allows high-privileged users to steal NTLM hash of Enterprise manager service account.	N/A	More Details
CVE-2024-29852	Veeam Backup Enterprise Manager allows high-privileged users to read backup session logs.	N/A	More Details
CVE-2024-29853	An authentication bypass vulnerability in Veeam Agent for Microsoft Windows allows for local privilege escalation.	N/A	More Details
CVE-2023-20239	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-35362	Ecshop 3.6 is vulnerable to Cross Site Scripting (XSS) via ecshop/article_cat.php.	N/A	More Details
CVE-2024-3708	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2021-47561	In the Linux kernel, the following vulnerability has been resolved: i2c: virtio: disable timeout handling If a timeout is hit, it can result is incorrect data on the I2C bus and/or memory corruptions in the guest since the device can still be operating on the buffers it was given while the guest has freed them. Here is, for example, the start of a slub_debug splat which was triggered on the next transfer after one transfer was forced to timeout by setting a breakpoint in the backend (rust-vmm/vhost-device): BUG kmalloc-1k (Not tainted): Poison overwritten First byte 0x1 instead of 0x6b Allocated in virtio_i2c_xfer+0x65/0x35c age=350 cpu=0 pid=29 __kmalloc+0xc2/0x1c9 virtio_i2c_xfer+0x65/0x35c __i2c_transfer+0x429/0x57d i2c_transfer+0x115/0x134 i2cdev_ioctl_rdwr+0x16a/0x1de i2cdev_ioctl+0x247/0x2ed vfs_ioctl+0x21/0x30 sys_ioctl+0xb18/0xb41 Freed in virtio_i2c_xfer+0x32e/0x35c age=244 cpu=0 pid=29 kfree+0x1bd/0x1cc virtio_i2c_xfer+0x32e/0x35c __i2c_transfer+0x429/0x57d i2c_transfer+0x115/0x134 i2cdev_ioctl_rdwr+0x16a/0x1de i2cdev_ioctl+0x247/0x2ed vfs_ioctl+0x21/0x30 sys_ioctl+0xb18/0xb41 There is no simple fix for this (the driver would have to always create bounce buffers and hold on to them until the device eventually returns the buffers), so just disable the timeout support for now.	N/A	More Details
CVE-2021-47560	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum: Protect driver from buggy firmware When processing port up/down events generated by the device's firmware, the driver protects itself from events reported for non-existent local ports, but not the CPU port (local port 0), which exists, but lacks a netdev. This can result in a NULL pointer dereference when calling netif_carrier_{on,off}(). Fix this by bailing early when processing an event reported for the CPU port. Problem was only observed when running on top of a buggy emulator.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47517	In the Linux kernel, the following vulnerability has been resolved: ethtool: do not perform operations on net devices being unregistered There is a short period between a net device starts to be unregistered and when it is actually gone. In that time frame ethtool operations could still be performed, which might end up in unwanted or undefined behaviours[1]. Do not allow ethtool operations after a net device starts its unregistration. This patch targets the netlink part as the ioctl one isn't affected: the reference to the net device is taken and the operation is executed within an rtnl lock section and the net device won't be found after unregister. [1] For example adding Tx queues after unregister ends up in NULL pointer exceptions and UaFs, such as: BUG: KASAN: use-after-free in kobject_get+0x14/0x90 Read of size 1 at addr ffff88801961248c by task ethtool/755 CPU: 0 PID: 755 Comm: ethtool Not tainted 5.15.0-rc6+ #778 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-4.fc34 04/014 Call Trace: dump_stack_lvl+0x57/0x72 print_address_description.constprop.0+0x1f/0x140 kasan_report.cold+0x7f/0x11b kobject_get+0x14/0x90 kobject_add_internal+0x3d1/0x450 kobject_init_and_add+0xba/0xf0 netdev_queue_update_kobjects+0xcf/0x200 netif_set_real_num_tx_queues+0xb4/0x310 veth_set_channels+0x1c3/0x550 ethnl_set_channels+0x524/0x610	N/A	More Details
CVE-2021-47531	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix mmap to include VM_IO and VM_DONTDUMP In commit 510410bfc034 ("drm/msm: Implement mmap as GEM object function") we switched to a new/cleaner method of doing things. That's good, but we missed a little bit. Before that commit, we used to _first_ run through the drm_gem_mmap_obj() case where `obj->funcs->mmap()` was NULL. That meant that we ran: vma->vm_flags |= VM_IO | VM_PFNMAP | VM_DONTEXPAND | VM_DONTDUMP; vma->vm_page_prot = pgprot_writecombine(vm_get_page_prot(vma->vm_flags)); vma->vm_page_prot = pgprot_decrypted(vma->vm_page_prot); ...and _then_ we modified those mappings with our own. Now that `obj->funcs->mmap()` is no longer NULL we don't run the default code. It looks like the fact that the vm_flags got VM_IO / VM_DONTDUMP was important because we're now getting crashes on Chromebooks that use ARC++ while logging out. Specifically a crash that looks like this (this is on a 5.10 kernel w/ relevant backports but also seen on a 5.15 kernel): Unable to handle kernel paging request at virtual address ffffffc008000000 Mem abort info: ESR = 0x96000006 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 Data abort info: ISV = 0, ISS = 0x00000006 CM = 0, WnR = 0 swapper pgtable: 4k pages, 39-bit VAs, pgdp=000000008293d000 [ffffffc008000000] pgd=00000001002b3003, p4d=00000001002b3003, pud=00000001002b3003, pmd=0000000000000000 Internal error: Oops: 96000006 [#1] PREEMPT SMP [...] CPU: 7 PID: 15734 Comm: crash_dump64 Tainted: G W 5.10.67 #1 [...] Hardware name: Qualcomm Technologies, Inc. sc7280 IDP SKU2 platform (DT) pstate: 80400009 (Nzcv daif +PAN -UAO -TCO BTYPE=--) pc : __arch_copy_to_user+0xc0/0x30c lr : copyout+0xac/0x14c [...] Call trace: __arch_copy_to_user+0xc0/0x30c copy_page_to_iter+0x1a0/0x294 process_vm_rw_core+0x240/0x408 process_vm_rw+0x110/0x16c __arm64_sys_process_vm_readv+0x30/0x3c el0_svc_common+0xf8/0x250 do_el0_svc+0x30/0x80 el0_svc+0x10/0x1c el0_sync_handler+0x78/0x108 el0_sync+0x184/0x1c0 Code: f8408423 f80008c3 910020c6 36100082 (b8404423) Let's add the two flags back in. While we're at it, the fact that we aren't running the default means that we _don't_ need to clear out VM_PFNMAP, so remove that and save an instruction. NOTE: it was confirmed that VM_IO was the important flag to fix the problem I was seeing, but adding back VM_DONTDUMP seems like a sane thing to do so I'm doing that too.	N/A	More Details
CVE-2021-47492	In the Linux kernel, the following vulnerability has been resolved: mm, thp: bail out early in collapse_file for writeback page Currently collapse_file does not explicitly check PG_writeback, instead, page_has_private and try_to_release_page are used to filter writeback pages. This does not work for xfs with blocksize equal to or larger than pagesize, because in such case xfs has no page->private. This makes collapse_file bail out early for writeback page. Otherwise, xfs end_page_writeback will panic as follows. page:fffffe00201bcc80 refcount:0 mapcount:0 mapping:ffff0003f88c86a8 index:0x0 pfn:0x84ef32 aops:xfs_address_space_operations [xfs] ino:30000b7 dentry name:"libtest.so" flags: 0x57fffe0000008027(lockedlreferencedluptodatelactivelwriteback) raw: 57fffe0000008027 ffff80001b48bc28 ffff80001b48bc28 ffff0003f88c86a8 raw: 0000000000000000 0000000000000000 00000000ffffffff ffff0000c3e9a000 page dumped because: VM_BUG_ON_PAGE(((unsigned int) page_ref_count(page) + 127u <= 127u)) page->mem_cgroup:ffff0000c3e9a000 ----------[cut here]---------- kernel BUG at include/linux/mm.h:1212! Internal error: Oops - BUG: 0 [#1] SMP Modules linked in: BUG: Bad page state in process khugepaged pfn:84ef32 xfs(E) page:fffffe00201bcc80 refcount:0 mapcount:0 mapping:0 index:0x0 pfn:0x84ef32 libcrc32c(E) rfkill(E) aes_ce_blk(E) crypto_simd(E) ... CPU: 25 PID: 0 Comm: swapper/25 Kdump: loaded Tainted: ... pstate: 60400005 (nZCv daif +PAN -UAO -TCO BTYPE=--) Call trace: end_page_writeback+0x1c0/0x214 iomap_finish_page_writeback+0x13c/0x204 iomap_finish_ioend+0xe8/0x19c iomap_writepage_end_bio+0x38/0x50 bio_endio+0x168/0x1ec blk_update_request+0x278/0x3f0 blk_mq_end_request+0x34/0x15c virtblk_request_done+0x38/0x74 [virtio_blk] blk_done_softirq+0xc4/0x110 __do_softirq+0x128/0x38c __irq_exit_rcu+0x118/0x150 irq_exit+0x1c/0x30 __handle_domain_irq+0x8c/0xf0 gic_handle_irq+0x84/0x108 el1_irq+0xcc/0x180 arch_cpu_idle+0x18/0x40 default_idle_call+0x4c/0x1a0 cpuidle_idle_call+0x168/0x1e0 do_idle+0xb4/0x104 cpu_startup_entry+0x30/0x9c secondary_start_kernel+0x104/0x180 Code: d4210000 b0006161 910c8021 94013f4d (d4210000) ---[end trace 4a88c6a074082f8c]--- Kernel panic - not syncing: Oops - BUG: Fatal exception in interrupt	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47491	In the Linux kernel, the following vulnerability has been resolved: mm: khugepaged: skip huge page collapse for special files The read-only THP for filesystems will collapse THP for files opened readonly and mapped with VM_EXEC. The intended usecase is to avoid TLB misses for large text segments. But it doesn't restrict the file types so a THP could be collapsed for a non-regular file, for example, block device, if it is opened readonly and mapped with EXEC permission. This may cause bugs, like [1] and [2]. This is definitely not the intended usecase, so just collapse THP for regular files in order to close the attack surface. [shy828301@gmail.com: fix vm_file check [3]]	N/A	More Details
CVE-2021-47490	In the Linux kernel, the following vulnerability has been resolved: drm/ttm: fix memleak in ttm_transfered_destroy We need to cleanup the fences for ghost objects as well. Bug: https://bugzilla.kernel.org/show_bug.cgi?id=214029 Bug: https://bugzilla.kernel.org/show_bug.cgi?id=214447	N/A	More Details
CVE-2021-47489	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix even more out of bound writes from debugfs CVE-2021-42327 was fixed by: commit f23750b5b3d98653b31d4469592935ef6364ad67 Author: Thelford Williams <tdwilliamsiv@gmail.com> Date: Wed Oct 13 16:04:13 2021 -0400 drm/amdgpu: fix out of bounds write but amdgpu_dm_debugfs.c contains more of the same issue so fix the remaining ones. v2: * Add missing fix in dp_max_bpc_write (Harry Wentland)	N/A	More Details
CVE-2021-47488	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2021-47487	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5410	Missing input validation in the ORing IAP-420 web-interface allows stored Cross-Site Scripting (XSS).This issue affects IAP-420 version 2.01e and below.	N/A	More Details
CVE-2024-5411	Missing input validation and OS command integration of the input in the ORing IAP-420 web-interface allows authenticated command injection.This issue affects IAP-420 version 2.01e and below.	N/A	More Details
CVE-2021-47530	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix wait_fence submitqueue leak We weren't dropping the submitqueue reference in all paths. In particular, when the fence has already been signalled. Split out a helper to simplify handling this in the various different return paths.	N/A	More Details
CVE-2024-0851	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Grup Arge Energy and Control Systems Smartpower allows SQL Injection.This issue affects Smartpower: through V24.05.27.	N/A	More Details
CVE-2021-47527	In the Linux kernel, the following vulnerability has been resolved: serial: core: fix transmit-buffer reset and memleak Commit 761ed4a94582 ("tty: serial_core: convert uart_close to use tty_port_close") converted serial core to use tty_port_close() but failed to notice that the transmit buffer still needs to be freed on final close. Not freeing the transmit buffer means that the buffer is no longer cleared on next open so that any ioctl() waiting for the buffer to drain might wait indefinitely (e.g. on termios changes) or that stale data can end up being transmitted in case tx is restarted. Furthermore, the buffer of any port that has been opened would leak on driver unbind. Note that the port lock is held when clearing the buffer pointer due to the ldisc race worked around by commit a5ba1d95e46e ("uart: fix race between uart_put_char() and uart_shutdown()"). Also note that the tty-port shutdown() callback is not called for console ports so it is not strictly necessary to free the buffer page after releasing the lock (cf. d72402145ace ("tty/serial: do not free trasnmit buffer page under port lock")).	N/A	More Details
CVE-2021-47485	In the Linux kernel, the following vulnerability has been resolved: IB/qib: Protect from buffer overflow in struct qib_user_sdma_pkt fields Overflowing either addrlimit or bytes_togo can allow userspace to trigger a buffer overflow of kernel memory. Check for overflows in all the places doing math on user controlled buffers.	N/A	More Details
CVE-2021-47524	In the Linux kernel, the following vulnerability has been resolved: serial: liteuart: fix minor-number leak on probe errors Make sure to release the allocated minor number before returning on probe errors.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47483	In the Linux kernel, the following vulnerability has been resolved: regmap: Fix possible double-free in regcache_rbtree_exit() In regcache_rbtree_insert_to_block(), when 'present' realloc failed, the 'blk' which is supposed to assign to 'rbnode->block' will be freed, so 'rbnode->block' points a freed memory, in the error handling path of regcache_rbtree_init(), 'rbnode->block' will be freed again in regcache_rbtree_exit(), KASAN will report double-free as follows: BUG: KASAN: double-free or invalid-free in kfree+0xce/0x390 Call Trace: slab_free_freelist_hook+0x10d/0x240 kfree+0xce/0x390 regcache_rbtree_exit+0x15d/0x1a0 regcache_rbtree_init+0x224/0x2c0 regcache_init+0x88d/0x1310 __regmap_init+0x3151/0x4a80 __devm_regmap_init+0x7d/0x100 madera_spi_probe+0x10f/0x333 [madera_spi] spi_probe+0x183/0x210 really_probe+0x285/0xc30 To fix this, moving up the assignment of rbnode->block to immediately after the reallocation has succeeded so that the data structure stays valid even if the second reallocation fails.	N/A	More Details
CVE-2021-47523	In the Linux kernel, the following vulnerability has been resolved: IB/hfi1: Fix leak of rcvhdrtail_dummy_kvaddr This buffer is currently allocated in hfi1_init(): if (reinit) ret = init_after_reset(dd); else ret = loadtime_init(dd); if (ret) goto done; /* allocate dummy tail memory for all receive contexts */ dd->rcvhdrtail_dummy_kvaddr = dma_alloc_coherent(&dd->pcidev->dev, sizeof(u64), &dd->rcvhdrtail_dummy_dma, GFP_KERNEL); if (!dd->rcvhdrtail_dummy_kvaddr) { dd_dev_err(dd, "cannot allocate dummy tail memory\n"); ret = -ENOMEM; goto done; } The reinit triggered path will overwrite the old allocation and leak it. Fix by moving the allocation to hfi1_alloc_devdata() and the deallocation to hfi1_free_devdata().	N/A	More Details
CVE-2021-47481	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Initialize the ODP xarray when creating an ODP MR Normally the zero fill would hide the missing initialization, but an errant set to desc_size in reg_create() causes a crash: BUG: unable to handle page fault for address: 0000000800000000 PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 5 PID: 890 Comm: ib_write_bw Not tainted 5.15.0-rc4+ #47 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 RIP: 0010:mlx5_ib_dereg_mr+0x14/0x3b0 [mlx5_ib] Code: 48 63 cd 4c 89 f7 48 89 0c 24 e8 37 30 03 e1 48 8b 0c 24 eb a0 90 0f 1f 44 00 00 41 56 41 55 41 54 55 53 48 89 fb 48 83 ec 30 <48> 8b 2f 65 48 8b 04 25 28 00 00 00 48 89 44 24 28 31 c0 8b 87 c8 RSP: 0018:ffff88811afa3a60 EFLAGS: 00010286 RAX: 000000000000001c RBX: 0000000800000000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000800000000 RBP: 0000000800000000 R08: 0000000000000000 R09: c0000000ffffff7f R10: ffff88811afa38f8 R11: ffff88811afa38f0 R12: ffffffffa02c7ac0 R13: 0000000000000000 R14: ffff88811afa3cd8 R15: ffff88810772fa00 FS: 00007f47b9080740(0000) GS:ffff88852cd40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000800000000 CR3: 000000010761e003 CR4: 0000000000370ea0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: mlx5_ib_free_odp_mr+0x95/0xc0 [mlx5_ib] mlx5_ib_dereg_mr+0x128/0x3b0 [mlx5_ib] ib_dereg_mr_user+0x45/0xb0 [ib_core] ? xas_load+0x8/0x80 destroy_hw_idr_uobject+0x1a/0x50 [ib_uverbs] uverbs_destroy_uobject+0x2f/0x150 [ib_uverbs] uobj_destroy+0x3c/0x70 [ib_uverbs] ib_uverbs_cmd_verbs+0x467/0xb00 [ib_uverbs] ? uverbs_finalize_object+0x60/0x60 [ib_uverbs] ? ttwu_queue_wakelist+0xa9/0xe0 ? pty_write+0x85/0x90 ? file_tty_write.isra.33+0x214/0x330 ? process_echoes+0x60/0x60 ib_uverbs_ioctl+0xa7/0x110 [ib_uverbs] __x64_sys_ioctl+0x10d/0x8e0 ? vfs_write+0x17f/0x260 do_syscall_64+0x3c/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae Add the missing xarray initialization and remove the desc_size set.	N/A	More Details
CVE-2021-47479	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8712: fix use-after-free in rtl8712_dl_fw Syzbot reported use-after-free in rtl8712_dl_fw(). The problem was in race condition between r871xu_dev_remove() ->ndo_open() callback. It's easy to see from crash log, that driver accesses released firmware in ->ndo_open() callback. It may happen, since driver was releasing firmware _before_ unregistering netdev. Fix it by moving unregister_netdev() before cleaning up resources. Call Trace: ... rtl871x_open_fw drivers/staging/rtl8712/hal_init.c:83 [inline] rtl8712_dl_fw+0xd95/0xe10 drivers/staging/rtl8712/hal_init.c:170 rtl8712_hal_init drivers/staging/rtl8712/hal_init.c:330 [inline] rtl871x_hal_init+0xae/0x180 drivers/staging/rtl8712/hal_init.c:394 netdev_open+0xe6/0x6c0 drivers/staging/rtl8712/os_intfs.c:380 __dev_open+0x2bc/0x4d0 net/core/dev.c:1484 Freed by task 1306: ... release_firmware+0x1b/0x30 drivers/base/firmware_loader/main.c:1053 r871xu_dev_remove+0xcc/0x2c0 drivers/staging/rtl8712/usb_intf.c:599 usb_unbind_interface+0x1d8/0x8d0 drivers/usb/core/driver.c:458	N/A	More Details
CVE-2024-3918	The Pet Manager WordPress plugin through 1.4 does not sanitise and escape some of its Pet settings, which could allow high privilege users such as Contributor to perform Stored Cross-Site Scripting attacks.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47493	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix race between searching chunks and release journal_head from buffer_head Encountered a race between ocfs2_test_bg_bit_allocatable() and jbd2_journal_put_journal_head() resulting in the below vmcore. PID: 106879 TASK: ffff880244ba9c00 CPU: 2 COMMAND: "loop3" Call trace: panic oops_end no_context __bad_area_nosemaphore bad_area_nosemaphore __do_page_fault do_page_fault page_fault [exception RIP: ocfs2_block_group_find_clear_bits+316] ocfs2_block_group_find_clear_bits [ocfs2] ocfs2_cluster_group_search [ocfs2] ocfs2_search_chain [ocfs2] ocfs2_claim_suballoc_bits [ocfs2] __ocfs2_claim_clusters [ocfs2] ocfs2_claim_clusters [ocfs2] ocfs2_local_alloc_slide_window [ocfs2] ocfs2_reserve_local_alloc_bits [ocfs2] ocfs2_reserve_clusters_with_limit [ocfs2] ocfs2_reserve_clusters [ocfs2] ocfs2_lock_refcount_allocators [ocfs2] ocfs2_make_clusters_writable [ocfs2] ocfs2_replace_cow [ocfs2] ocfs2_refcount_cow [ocfs2] ocfs2_file_write_iter [ocfs2] lo_rw_aio loop_queue_work kthread_worker_fn kthread ret_from_fork When ocfs2_test_bg_bit_allocatable() called bh2jh(bg_bh), the bg_bh->b_private NULL as jbd2_journal_put_journal_head() raced and released the jounal head from the buffer head. Needed to take bit lock for the bit 'BH_JournalHead' to fix this race.	N/A	More Details
CVE-2024-29078	Incorrect permission assignment for critical resource issue exists in MosP kintai kanri V4.6.6 and earlier, which may allow a remote unauthenticated attacker with access to the product to alter the product settings.	N/A	More Details
CVE-2021-47494	In the Linux kernel, the following vulnerability has been resolved: cfg80211: fix management registrations locking The management registrations locking was broken, the list was locked for each wdev, but cfg80211_mgmt_registrations_update() iterated it without holding all the correct spinlocks, causing list corruption. Rather than trying to fix it with fine-grained locking, just move the lock to the wiphy/rdev (still need the list on each wdev), we already need to hold the wdev lock to change it, so there's no contention on the lock in any case. This trivially fixes the bug since we hold one wdev's lock already, and now will hold the lock that protects all lists.	N/A	More Details
CVE-2021-47495	In the Linux kernel, the following vulnerability has been resolved: usbnet: sanity check for maxpacket maxpacket of 0 makes no sense and oopses as we need to divide by it. Give up. V2: fixed typo in log and stylistic issues	N/A	More Details
CVE-2021-47558	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: Disable Tx queues when reconfiguring the interface The Tx queues were not disabled in situations where the driver needed to stop the interface to apply a new configuration. This could result in a kernel panic when doing any of the 3 following actions: * reconfiguring the number of queues (ethtool -L) * reconfiguring the size of the ring buffers (ethtool -G) * installing/removing an XDP program (ip l set dev ethX xdp) Prevent the panic by making sure netif_tx_disable is called when stopping an interface. Without this patch, the following kernel panic can be observed when doing any of the actions above: Unable to handle kernel paging request at virtual address ffff80001238d040 [....] Call trace: dwmac4_set_addr+0x8/0x10 dev_hard_start_xmit+0xe4/0x1ac sch_direct_xmit+0xe8/0x39c __dev_queue_xmit+0x3ec/0xaf0 dev_queue_xmit+0x14/0x20 [...] [end trace 0000000000000002]---	N/A	More Details
CVE-2024-4153	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-2021-47557	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_ets: don't peek at classes beyond 'nbands' when the number of DRR classes decreases, the round-robin active list can contain elements that have already been freed in ets_qdisc_change(). As a consequence, it's possible to see a NULL dereference crash, caused by the attempt to call cl->qdisc->ops->peek(cl->qdisc) when cl->qdisc is NULL: BUG: kernel NULL pointer dereference, address: 0000000000000018 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 1 PID: 910 Comm: mausezahn Not tainted 5.16.0-rc1+ #475 Hardware name: Red Hat KVM, BIOS 1.11.1-4.module+el8.1.0+4066+0f1aadab 04/01/2014 RIP: 0010:ets_qdisc_dequeue+0x129/0x2c0 [sch_ets] Code: c5 01 41 39 ad e4 02 00 00 0f 87 18 ff ff ff 49 8b 85 c0 02 00 00 49 39 c4 0f 84 ba 00 00 00 49 8b ad c0 02 00 00 48 8b 7d 10 <48> 8b 47 18 48 8b 40 38 0f ae e8 ff d0 48 89 c3 48 85 c0 0f 84 9d RSP: 0000:ffffbb36c0b5fdd8 EFLAGS: 00010287 RAX: ffff956678efed30 RBX: 0000000000000000 RCX: 0000000000000000 RDX: 0000000000000002 RSI: ffffffff9b938dc9 RDI: 0000000000000000 RBP: ffff956678efed30 R08: e2f3207fe360129c R09: 0000000000000000 R10: 0000000000000001 R11: 0000000000000001 R12: ffff956678efeac0 R13: ffff956678efe800 R14: ffff956611545000 R15: ffff95667ac8f100 FS: 00007f2aa9120740(0000) GS:ffff95667b800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000018 CR3: 000000011070c000 CR4: 0000000000350ee0 Call Trace: <TASK> qdisc_peek_dequeued+0x29/0x70 [sch_ets] tbf_dequeue+0x22/0x260 [sch_tbf] __qdisc_run+0x7f/0x630 net_tx_action+0x290/0x4c0 __do_softirq+0xee/0x4f8 irq_exit_rcu+0xf4/0x130 sysvec_apic_timer_interrupt+0x52/0xc0 asm_sysvec_apic_timer_interrupt+0x12/0x20 RIP: 0033:0x7f2aa7fc9ad4 Code: b9 ff ff 48 8b 54 24 18 48 83 c4 08 48 89 ee 48 89 df 5b 5d e9 ed fc ff ff 0f 1f 00 66 2e 0f 1f 84 00 00 00 00 00 f3 0f 1e fa <53> 48 83 ec 10 48 8b 05 10 64 33 00 48 8b 00 48 85 c0 0f 85 84 00 RSP: 002b:00007ffe5d33fab8 EFLAGS: 00000202 RAX: 0000000000000002 RBX: 0000561f72c31460 RCX: 0000561f72c31720 RDX: 0000000000000002 RSI: 0000561f72c31722 RDI: 0000561f72c31720 RBP: 000000000000002a R08: 00007ffe5d33fa40 R09: 0000000000000014 R10: 0000000000000000 R11: 0000000000000246 R12: 0000561f7187e380 R13: 0000000000000000 R14: 0000000000000000 R15: 0000561f72c31460 </TASK> Modules linked in: sch_ets sch_tbf dummy rfkill iTCO_wdt intel_rapl_msr iTCO_vendor_support intel_rapl_common joydev virtio_balloon lpc_ich i2c_i801 i2c_smbus pcspkr ip_tables xfs libcrc32c crct10dif_pclmul crc32_pclmul crc32c_intel ahci libahci ghash_clmulni_intel serio_raw libata virtio_blk virtio_console virtio_net net_failover failover sunrpc dm_mirror dm_region_hash dm_log dm_mod CR2: 0000000000000018 Ensuring that 'alist' was never zeroed [1] was not sufficient, we need to remove from the active list those elements that are no more SP nor DRR. [1] https://lore.kernel.org/netdev/60d274838bf09777f0371253416e8af71360bc08.1633609148.git.dcaratti@redhat.com/ v3: fix race between ets_qdisc_change() and ets_qdisc_dequeue() delisting DRR classes beyond 'nbands' in ets_qdisc_change() with the qdisc lock acquired, thanks to Cong Wang. v2: when a NULL qdisc is found in the DRR active list, try to dequeue skb from the next list item.	N/A	More Details
CVE-2021-47554	In the Linux kernel, the following vulnerability has been resolved: vdpa_sim: avoid putting an uninitialized iova_domain The system will crash if we put an uninitialized iova_domain, this could happen when an error occurs before initializing the iova_domain in vdpasim_create(). BUG: kernel NULL pointer dereference, address: 0000000000000000 ... RIP: 0010:__cpuhp_state_remove_instance+0x96/0x1c0 ... Call Trace: <TASK> put_iova_domain+0x29/0x220 vdpasim_free+0xd1/0x120 [vdpa_sim] vdpa_release_dev+0x21/0x40 [vdpa] device_release+0x33/0x90 kobject_release+0x63/0x160 vdpasim_create+0x127/0x2a0 [vdpa_sim] vdpasim_net_dev_add+0x7d/0xfe [vdpa_sim_net] vdpa_nl_cmd_dev_add_set_doit+0xe1/0x1a0 [vdpa] genl_family_rcv_msg_doit+0x112/0x140 genl_rcv_msg+0xdf/0x1d0 ... So we must make sure the iova_domain is already initialized before put it. In addition, we may get the following warning in this case: WARNING: ... drivers/iommu/iova.c:344 iova_cache_put+0x58/0x70 So we must make sure the iova_cache_put() is invoked only if the iova_cache_get() is already invoked. Let's fix it together.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47553	In the Linux kernel, the following vulnerability has been resolved: sched/scs: Reset task stack state in bringup_cpu() To hot unplug a CPU, the idle task on that CPU calls a few layers of C code before finally leaving the kernel. When KASAN is in use, poisoned shadow is left around for each of the active stack frames, and when shadow call stacks are in use. When shadow call stacks (SCS) are in use the task's saved SCS SP is left pointing at an arbitrary point within the task's shadow call stack. When a CPU is offlined than onlined back into the kernel, this stale state can adversely affect execution. Stale KASAN shadow can alias new stackframes and result in bogus KASAN warnings. A stale SCS SP is effectively a memory leak, and prevents a portion of the shadow call stack being used. Across a number of hotplug cycles the idle task's entire shadow call stack can become unusable. We previously fixed the KASAN issue in commit: e1b77c92981a5222 ("sched/kasan: remove stale KASAN poison after hotplug") ... by removing any stale KASAN stack poison immediately prior to onlining a CPU. Subsequently in commit: f1a0a376ca0c4ef1 ("sched/core: Initialize the idle task with preemption disabled") ... the refactoring left the KASAN and SCS cleanup in one-time idle thread initialization code rather than something invoked prior to each CPU being onlined, breaking both as above. We fixed SCS (but not KASAN) in commit: 63acd42c0d4942f7 ("sched/scs: Reset the shadow stack when idle_task_exit") ... but as this runs in the context of the idle task being offlined it's potentially fragile. To fix these consistently and more robustly, reset the SCS SP and KASAN shadow of a CPU's idle task immediately before we online that CPU in bringup_cpu(). This ensures the idle task always has a consistent state when it is running, and removes the need to so so when exiting an idle task. Whenever any thread is created, dup_task_struct() will give the task a stack which is free of KASAN shadow, and initialize the task's SCS SP, so there's no need to specially initialize either for idle thread within init_idle(), as this was only necessary to handle hotplug cycles. I've tested this on arm64 with: * gcc 11.1.0, defconfig +KASAN_INLINE, KASAN_STACK * clang 12.0.0, defconfig +KASAN_INLINE, KASAN_STACK, SHADOW_CALL_STACK ... offlining and onlining CPUS with: l while true; do l for C in /sys/devices/system/cpu/cpu*/online; do l echo 0 > $C; l echo 1 > $C; l done l done	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47552	In the Linux kernel, the following vulnerability has been resolved: blk-mq: cancel blk-mq dispatch work in both blk_cleanup_queue and disk_release() For avoiding to slow down queue destroy, we don't call blk_mq_quiesce_queue() in blk_cleanup_queue(), instead of delaying to cancel dispatch work in blk_release_queue(). However, this way has caused kernel oops[1], reported by Changhui. The log shows that scsi_device can be freed before running blk_release_queue(), which is expected too since scsi_device is released after the scsi disk is closed and the scsi_device is removed. Fixes the issue by canceling blk-mq dispatch work in both blk_cleanup_queue() and disk_release(): 1) when disk_release() is run, the disk has been closed, and any sync dispatch activities have been done, so canceling dispatch work is enough to quiesce filesystem I/O dispatch activity. 2) in blk_cleanup_queue(), we only focus on passthrough request, and passthrough request is always explicitly allocated & freed by its caller, so once queue is frozen, all sync dispatch activity for passthrough request has been done, then it is enough to just cancel dispatch work for avoiding any dispatch activity. [1] kernel panic log [12622.769416] BUG: kernel NULL pointer dereference, address: 0000000000000300 [12622.777186] #PF: supervisor read access in kernel mode [12622.782918] #PF: error_code(0x0000) - not-present page [12622.788649] PGD 0 P4D 0 [12622.791474] Oops: 0000 [#1] PREEMPT SMP PTI [12622.796138] CPU: 10 PID: 744 Comm: kworker/10:1H Kdump: loaded Not tainted 5.15.0+ #1 [12622.804877] Hardware name: Dell Inc. PowerEdge R730/0H21J3, BIOS 1.5.4 10/002/2015 [12622.813321] Workqueue: kblockd blk_mq_run_work_fn [12622.818572] RIP: 0010:sbitmap_get+0x75/0x190 [12622.823336] Code: 85 80 00 00 00 41 8b 57 08 85 d2 0f 84 b1 00 00 00 45 31 e4 48 63 cd 48 8d 1c 49 48 c1 e3 06 49 03 5f 10 4c 8d 6b 40 83 f0 01 <48> 8b 33 44 89 f2 4c 89 ef 0f b6 c8 e8 fa f3 ff ff 83 f8 ff 75 58 [12622.844290] RSP: 0018:ffffb00a446dbd40 EFLAGS: 00010202 [12622.850120] RAX: 0000000000000001 RBX: 0000000000000300 RCX: 0000000000000004 [12622.858082] RDX: 0000000000000006 RSI: 0000000000000082 RDI: ffffa0b7a2dfe030 [12622.866042] RBP: 0000000000000004 R08: 0000000000000001 R09: ffffa0b742721334 [12622.874003] R10: 0000000000000008 R11: 0000000000000008 R12: 0000000000000000 [12622.881964] R13: 0000000000000340 R14: 0000000000000000 R15: ffffa0b7a2dfe030 [12622.889926] FS: 0000000000000000(0000) GS:ffffa0baafb40000(0000) knlGS:0000000000000000 [12622.898956] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [12622.905367] CR2: 0000000000000300 CR3: 0000000641210001 CR4: 00000000001706e0 [12622.913328] Call Trace: [12622.916055] <TASK> [12622.918394] scsi_mq_get_budget+0x1a/0x110 [12622.922969] __blk_mq_do_dispatch_sched+0x1d4/0x320 [12622.928404] ? pick_next_task_fair+0x39/0x390 [12622.933268] __blk_mq_sched_dispatch_requests+0xf4/0x140 [12622.939194] blk_mq_sched_dispatch_requests+0x30/0x60 [12622.944829] __blk_mq_run_hw_queue+0x30/0xa0 [12622.949593] process_one_work+0x1e8/0x3c0 [12622.954059] worker_thread+0x50/0x3b0 [12622.958144] ? rescuer_thread+0x370/0x370 [12622.962616] kthread+0x158/0x180 [12622.966218] ? set_kthread_struct+0x40/0x40 [12622.970884] ret_from_fork+0x22/0x30 [12622.974875] </TASK> [12622.977309] Modules linked in: scsi_debug rpcsec_gss_krb5 auth_rpcgss nfsv4 dns_resolver nfs lockd grace fscache netfs sunrpc dm_multipath intel_rapl_msr intel_rapl_common dell_wmi_descriptor sb_edac rfkill video x86_pkg_temp_thermal intel_powerclamp dcdbas coretemp kvm_intel kvm mgag200 irqbypass i2c_algo_bit rapl drm_kms_helper ipmi_ssif intel_cstate intel_uncore syscopyarea sysfillrect sysimgblt fb_sys_fops pcspkr cec mei_me lpc_ich mei ipmi_si ipmi_devintf ipmi_msghandler acpi_power_meter drm fuse xfs libcrc32c sr_mod cdrom sd_mod t10_pi sg ixgbe ahci libahci crct10dif_pclmul crc32_pclmul crc32c_intel libata megaraid_sas ghash_clmulni_intel tg3 wdat_w ---truncated---	N/A	More Details
CVE-2021-47549	In the Linux kernel, the following vulnerability has been resolved: sata_fsl: fix UAF in sata_fsl_port_stop when rmmod sata_fsl When the `rmmod sata_fsl.ko` command is executed in the PPC64 GNU/Linux, a bug is reported: == BUG: Unable to handle kernel data access on read at 0x80000800805b502c Oops: Kernel access of bad area, sig: 11 [#1] NIP [c0000000000388a4] .ioread32+0x4/0x20 LR [80000000000c6034] .sata_fsl_port_stop+0x44/0xe0 [sata_fsl] Call Trace: .free_irq+0x1c/0x4e0 (unreliable) .ata_host_stop+0x74/0xd0 [libata] .release_nodes+0x330/0x3f0 .device_release_driver_internal+0x178/0x2c0 .driver_detach+0x64/0xd0 .bus_remove_driver+0x70/0xf0 .driver_unregister+0x38/0x80 .platform_driver_unregister+0x14/0x30 .fsl_sata_driver_exit+0x18/0xa20 [sata_fsl] .__se_sys_delete_module+0x1ec/0x2d0 .system_call_exception+0xfc/0x1f0 system_call_common+0xf8/0x200 == The triggering of the BUG is shown in the following stack: driver_detach device_release_driver_internal __device_release_driver drv->remove(dev) --> platform_drv_remove/platform_remove drv->remove(dev) --> sata_fsl_remove iounmap(host_priv->hcr_base); <---- unmap kfree(host_priv); <---- free devres_release_all release_nodes dr->node.release(dev, dr->data) --> ata_host_stop ap->ops->port_stop(ap) --> sata_fsl_port_stop ioread32(hcr_base + HCONTROL) <---- UAF host->ops->host_stop(host) The iounmap(host_priv->hcr_base) and kfree(host_priv) functions should not be executed in drv->remove. These functions should be executed in host_stop after port_stop. Therefore, we move these functions to the new function sata_fsl_host_stop and bind the new function to host_stop.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47545	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2021-47544	In the Linux kernel, the following vulnerability has been resolved: tcp: fix page frag corruption on page fault Steffen reported a TCP stream corruption for HTTP requests served by the apache web-server using a cifs mount-point and memory mapping the relevant file. The root cause is quite similar to the one addressed by commit 20eb4f29b602 ("net: fix sk_page_frag() recursion from memory reclaim"). Here the nested access to the task page frag is caused by a page fault on the (mmapped) user-space memory buffer coming from the cifs file. The page fault handler performs an smb transaction on a different socket, inside the same process context. Since sk->sk_allaction for such socket does not prevent the usage for the task_frag, the nested allocation modify "under the hood" the page frag in use by the outer sendmsg call, corrupting the stream. The overall relevant stack trace looks like the following: httpd 78268 [001] 3461630.850950: probe:tcp_sendmsg_locked: ffffffff91461d91 tcp_sendmsg_locked+0x1 ffffffff91462b57 tcp_sendmsg+0x27 ffffffff9139814e sock_sendmsg+0x3e ffffffffc06dfe1d smb_send_kvec+0x28 [...] ffffffffc06cfaf8 cifs_readpages+0x213 ffffffff90e83c4b read_pages+0x6b ffffffff90e83f31 __do_page_cache_readahead+0x1c1 ffffffff90e79e98 filemap_fault+0x788 ffffffff90eb0458 __do_fault+0x38 ffffffff90eb5280 do_fault+0x1a0 ffffffff90eb7c84 __handle_mm_fault+0x4d4 ffffffff90eb8093 handle_mm_fault+0xc3 ffffffff90c74f6d __do_page_fault+0x1ed ffffffff90c75277 do_page_fault+0x37 ffffffff9160111e page_fault+0x1e ffffffff9109e7b5 copyin+0x25 ffffffff9109eb40 _copy_from_iter_full+0xe0 ffffffff91462370 tcp_sendmsg_locked+0x5e0 ffffffff91462370 tcp_sendmsg_locked+0x5e0 ffffffff91462b57 tcp_sendmsg+0x27 ffffffff9139815c sock_sendmsg+0x4c ffffffff913981f7 sock_write_iter+0x97 ffffffff90f2cc56 do_iter_readv_writev+0x156 ffffffff90f2dff0 do_iter_write+0x80 ffffffff90f2e1c3 vfs_writev+0xa3 ffffffff90f2e27c do_writev+0x5c ffffffff90c042bb do_syscall_64+0x5b ffffffff916000ad entry_SYSCALL_64_after_hwframe+0x65 The cifs filesystem rightfully sets sk_allocations to GFP_NOFS, we can avoid the nesting using the sk page frag for allocation lacking the __GFP_FS flag. Do not define an additional mm-helper for that, as this is strictly tied to the sk page frag usage. v1 -> v2: - use a stricted sk_page_frag() check instead of reordering the code (Eric)	N/A	More Details
CVE-2021-47543	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2021-47539	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix rxrpc_peer leak in rxrpc_look_up_bundle() Need to call rxrpc_put_peer() for bundle candidate before kfree() as it holds a ref to rxrpc_peer. [DH: v2: Changed to abstract out the bundle freeing code into a function]	N/A	More Details
CVE-2021-47538	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix rxrpc_local leak in rxrpc_lookup_peer() Need to call rxrpc_put_local() for peer candidate before kfree() as it holds a ref to rxrpc_local. [DH: v2: Changed to abstract the peer freeing code out into a function]	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47536	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix wrong list_del in smc_lgr_cleanup_early smc_lgr_cleanup_early() meant to delete the link group from the link group list, but it deleted the list head by mistake. This may cause memory corruption since we didn't remove the real link group from the list and later memseted the link group structure. We got a list corruption panic when testing: [231.277259] list_del corruption. prev->next should be ffff8881398a8000, but was 0000000000000000 [231.278222] ------------[cut here]------------ [231.278726] kernel BUG at lib/list_debug.c:53! [231.279326] invalid opcode: 0000 [#1] SMP NOPTI [231.279803] CPU: 0 PID: 5 Comm: kworker/0:0 Not tainted 5.10.46+ #435 [231.280466] Hardware name: Alibaba Cloud ECS, BIOS 8c24b4c 04/01/2014 [231.281248] Workqueue: events smc_link_down_work [231.281732] RIP: 0010:__list_del_entry_valid+0x70/0x90 [231.282258] Code: 4c 60 82 e8 7d cc 6a 00 0f 0b 48 89 fe 48 c7 c7 88 4c 60 82 e8 6c cc 6a 00 0f 0b 48 89 fe 48 c7 c7 c0 4c 60 82 e8 5b cc 6a 00 <0f> 0b 48 89 fe 48 c7 c7 00 4d 60 82 e8 4a cc 6a 00 0f 0b cc cc cc [231.284146] RSP: 0018:ffffc90000033d58 EFLAGS: 00010292 [231.284685] RAX: 0000000000000054 RBX: ffff8881398a8000 RCX: 0000000000000000 [231.285415] RDX: 0000000000000001 RSI: ffff88813bc18040 RDI: ffff88813bc18040 [231.286141] RBP: ffffffff8305ad40 R08: 0000000000000003 R09: 0000000000000001 [231.286873] R10: ffffffff82803da0 R11: ffffc90000033b90 R12: 0000000000000001 [231.287606] R13: 0000000000000000 R14: ffff8881398a8000 R15: 0000000000000003 [231.288337] FS: 0000000000000000(0000) GS:ffff88813bc00000(0000) knlGS:0000000000000000 [231.289160] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [231.289754] CR2: 0000000000e72058 CR3: 000000010fa96006 CR4: 00000000003706f0 [231.290485] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [231.291211] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [231.291940] Call Trace: [231.292211] smc_lgr_terminate_sched+0x53/0xa0 [231.292677] smc_switch_conns+0x75/0x6b0 [231.293085] ? update_load_avg+0x1a6/0x590 [231.293517] ? ttwu_do_wakeup+0x17/0x150 [231.293907] ? update_load_avg+0x1a6/0x590 [231.294317] ? newidle_balance+0xca/0x3d0 [231.294716] smcr_link_down+0x50/0x1a0 [231.295090] ? __wake_up_common_lock+0x77/0x90 [231.295534] smc_link_down_work+0x46/0x60 [231.295933] process_one_work+0x18b/0x350	N/A	More Details
CVE-2021-47533	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: kms: Clear the HVS FIFO commit pointer once done Commit 9ec03d7f1ed3 ("drm/vc4: kms: Wait on previous FIFO users before a commit") introduced a wait on the previous commit done on a given HVS FIFO. However, we never cleared that pointer once done. Since drm_crtc_commit_put can free the drm_crtc_commit structure directly if we were the last user, this means that it can lead to a use-after free if we were to duplicate the state, and that stale pointer would even be copied to the new state. Set the pointer to NULL once we're done with the wait so that we don't carry over a pointer to a free'd structure.	N/A	More Details
CVE-2021-47497	In the Linux kernel, the following vulnerability has been resolved: nvmem: Fix shift-out-of-bound (UBSAN) with byte size cells If a cell has 'nbits' equal to a multiple of BITS_PER_BYTE the logic *p &= GENMASK((cell->nbits%BITS_PER_BYTE) - 1, 0); will become undefined behavior because nbits modulo BITS_PER_BYTE is 0, and we subtract one from that making a large number that is then shifted more than the number of bits that fit into an unsigned long. UBSAN reports this problem: UBSAN: shift-out-of-bounds in drivers/nvmem/core.c:1386:8 shift exponent 64 is too large for 64-bit type 'unsigned long' CPU: 6 PID: 7 Comm: kworker/u16:0 Not tainted 5.15.0-rc3+ #9 Hardware name: Google Lazor (rev3+) with KB Backlight (DT) Workqueue: events_unbound deferred_probe_work_func Call trace: dump_backtrace+0x0/0x170 show_stack+0x24/0x30 dump_stack_lvl+0x64/0x7c dump_stack+0x18/0x38 ubsan_epilogue+0x10/0x54 __ubsan_handle_shift_out_of_bounds+0x180/0x194 __nvmem_cell_read+0x1ec/0x21c nvmem_cell_read+0x58/0x94 nvmem_cell_read_variable_common+0x4c/0xb0 nvmem_cell_read_variable_le_u32+0x40/0x100 a6xx_gpu_init+0x170/0x2f4 adreno_bind+0x174/0x284 component_bind_all+0xf0/0x264 msm_drm_bind+0x1d8/0x7a0 try_to_bring_up_master+0x164/0x1ac __component_add+0xbc/0x13c component_add+0x20/0x2c dp_display_probe+0x340/0x384 platform_probe+0xc0/0x100 really_probe+0x110/0x304 __driver_probe_device+0xb8/0x120 driver_probe_device+0x4c/0xfc __device_attach_driver+0xb0/0x128 bus_for_each_drv+0x90/0xdc __device_attach+0xc8/0x174 device_initial_probe+0x20/0x2c bus_probe_device+0x40/0xa4 deferred_probe_work_func+0x7c/0xb8 process_one_work+0x128/0x21c process_scheduled_works+0x40/0x54 worker_thread+0x1ec/0x2a8 kthread+0x138/0x158 ret_from_fork+0x10/0x20 Fix it by making sure there are any bits to mask out.	N/A	More Details
CVE-2021-47532	In the Linux kernel, the following vulnerability has been resolved: drm/msm/devfreq: Fix OPP refcnt leak	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47496	In the Linux kernel, the following vulnerability has been resolved: net/tls: Fix flipped sign in tls_err_abort() calls sk->sk_err appears to expect a positive value, a convention that ktls doesn't always follow and that leads to memory corruption in other code. For instance, [kworker] tls_encrypt_done(..., err=<negative error from crypto request>) tls_err_abort(.., err) sk->sk_err = err; [task] splice_from_pipe_feed ... tls_sw_do_sendpage if (sk->sk_err) { ret = -sk->sk_err; // ret is positive splice_from_pipe_feed (continued) ret = actor(...) // ret is still positive and interpreted as bytes // written, resulting in underflow of buf->len and // sd->len, leading to huge buf->offset and bogus // addresses computed in later calls to actor() Fix all tls_err_abort() callers to pass a negative error code consistently and centralize the error-prone sign flip there, throwing in a warning to catch future misuse and uninlining the function so it really does only warn once.	N/A	More Details
CVE-2021-47499	In the Linux kernel, the following vulnerability has been resolved: iio: accel: kxcjk-1013: Fix possible memory leak in probe and remove When ACPI type is ACPI_SMO8500, the data->dready_trig will not be set, the memory allocated by iio_triggered_buffer_setup() will not be freed, and cause memory leak as follows: unreferenced object 0xffff888009551400 (size 512): comm "i2c-SMO8500-125", pid 911, jiffies 4294911787 (age 83.852s) hex dump (first 32 bytes): 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 20 e2 e5 c0 ff ff ff ff .... backtrace: [<0000000041ce75ee>] kmem_cache_alloc_trace+0x16d/0x360 [<000000000aeb17b0>] iio_kfifo_allocate+0x41/0x130 [kfifo_buf] [<000000004b40c1f5>] iio_triggered_buffer_setup_ext+0x2c/0x210 [industrialio_triggered_buffer] [<000000004375b15f>] kxcjk1013_probe+0x10c3/0x1d81 [kxcjk_1013] Fix it by remove data->dready_trig condition in probe and remove.	N/A	More Details