SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 01 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-2024-32766 | An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later | 10.0 | More Details |
| CVE-2024-32651 | changedetection.io is an open source web page change detection, website watcher, restock monitor and notification service. There is a Server Side Template Injection (SSTI) in Jinja2 that allows Remote Command Execution on the server host. Attackers can run any system command without any restriction and they could use a reverse shell. The impact is critical as the attacker can completely takeover the server machine. This can be reduced if changedetection is behind a login page, but this isn't required by the application (not by default and not enforced). | 10.0 | More Details |
| CVE-2024-0916 | Unauthenticated file upload allows remote code execution. This issue affects UvDesk Community: from 1.0.0 through 1.1.3. | 10.0 | More Details |
| CVE-2024-33566 | Missing Authorization vulnerability in N-Media OrderConvo allows OS Command Injection.This issue affects OrderConvo: from n/a through 12.4. | 10.0 | More Details |
| CVE-2023-51482 | Improper Authentication vulnerability in EazyPlugins Eazy Plugin Manager allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Eazy Plugin Manager: from n/a through 4.1.2. | 9.9 | More Details |
| CVE-2024-32764 | A missing authentication for critical function vulnerability has been reported to affect myQNAPcloud Link. If exploited, the vulnerability could allow users with the privilege level of some functionality via a network. We have already fixed the vulnerability in the following version: myQNAPcloud Link 2.4.51 and later | 9.9 | More Details |
| CVE-2024-3342 | The Timetable and Event Schedule by MotoPress plugin for WordPress is vulnerable to SQL Injection via the 'events' attribute of the 'mp-timetable' shortcode in all versions up to, and including, 2.4.11 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. | 9.9 | More Details |
| CVE-2023-31090 | Unrestricted Upload of File with Dangerous Type vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Upload a Web Shell to a Web Server.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.60. | 9.9 | More Details |
| CVE-2024-4306 | Critical unrestricted file upload vulnerability in HubBank affecting version 1.0.2. This vulnerability allows a registered user to upload malicious PHP files via upload document fields, resulting in webshell execution. | 9.9 | More Details |
| CVE-2024-31820 | An issue in Ecommerce-CodeIgniter-Bootstrap commit v. d22b54e8915f167a135046ceb857caaf8479c4da allows a remote attacker to execute arbitrary code via the getLangFolderForEdit method of the Languages.php component. | 9.8 | More Details |
| CVE-2024-33445 | An issue in hisiphp v2.0.111 allows a remote attacker to execute arbitrary code via a crafted script to the SystemPlugins::mkInfo parameter in the SystemPlugins.php component. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-33268 | SQL Injection vulnerability in Digincube mdgiftproduct before 1.4.1 allows an attacker to run arbitrary SQL commands via the MdGiftRule::addGiftToCart method. | 9.8 | More Details |
| CVE-2024-33350 | Directory Traversal vulnerability in TaoCMS v.3.0.2 allows a remote attacker to execute arbitrary code and obtain sensitive information via the include/model/file.php component. | 9.8 | More Details |
| CVE-2024-31601 | An issue in Beijing Panabit Network Software Co., Ltd Panalog big data analysis platform v. 20240323 and before allows attackers to execute arbitrary code via the exportpdf.php component. | 9.8 | More Details |
| CVE-2024-32881 | Danswer is the AI Assistant connected to company's docs, apps, and people. Danswer is vulnerable to unauthorized access to GET/SET of Slack Bot Tokens. Anyone with network access can steal slack bot tokens and set them. This implies full compromise of the customer's slack bot, leading to internal Slack access. This issue was patched in version 3.63. | 9.8 | More Details |
| CVE-2024-28322 | SQL Injection vulnerability in /event-management-master/backend/register.php in PuneethReddyHC Event Management 1.0 allows attackers to run arbitrary SQL commands via the event_id parameter in a crafted POST request. | 9.8 | More Details |
| CVE-2024-30804 | An issue discovered in the DeviceIoControl component in ASUS Fan_Xpert before v.10013 allows an attacker to execute arbitrary code via crafted IOCTL requests. | 9.8 | More Details |
| CVE-2024-4300 | E-WEBInformationCo. FS-EZViewer(Web) exposes sensitive information in the service. A remote attacker can obtain the database configuration file path through the webpage source code without login. Accessing this path allows attacker to obtain the database credential with the highest privilege and database host IP address. With this information, attackers can connect to the database and perform actions such as adding, modifying, or deleting database contents. | 9.8 | More Details |
| CVE-2024-33266 | SQL Injection vulnerability in Helloshop deliveryorderautoupdate v.2.8.1 and before allows an attacker to run arbitrary SQL commands via the DeliveryorderautoupdateOrdersModuleFrontController::initContent function. | 9.8 | More Details |
| CVE-2024-33449 | An SSRF issue in the PDFMyURL service allows a remote attacker to obtain sensitive information and execute arbitrary code via a POST request in the url parameter | 9.8 | More Details |
| CVE-2024-3191 | A vulnerability, which was classified as critical, has been found in MailCleaner up to 2023.03.14. This issue affects some unknown processing of the component Email Handler. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-262307. | 9.8 | More Details |
| CVE-2024-33435 | Insecure Permissions vulnerability in Guangzhou Yingshi Electronic Technology Co. Ncast Yingshi high-definition intelligent recording and playback system 2007-2017 allows a remote attacker to execute arbitrary code via the /manage/IPSetup.php backend function | 9.8 | More Details |
| CVE-2024-31822 | An issue in Ecommerce-CodeIgniter-Bootstrap commit v. d22b54e8915f167a135046ceb857caaf8479c4da allows a remote attacker to execute arbitrary code via the saveLanguageFiles method of the Languages.php component. | 9.8 | More Details |
| CVE-2024-33276 | SQL Injection vulnerability in FME Modules preorderandnotication v.3.1.0 and before allows a remote attacker to run arbitrary SQL commands via the PreorderModel::getIdProductAttributesByIdAttributes() method. | 9.8 | More Details |
| CVE-2024-32491 | An issue was discovered in Znuny and Znuny LTS 6.0.31 through 6.5.7 and Znuny 7.0.1 through 7.0.16 where a logged-in user can upload a file (via a manipulated AJAX Request) to an arbitrary writable location by traversing paths. Arbitrary code can be executed if this location is publicly available through the web server. | 9.8 | More Details |
| CVE-2024-33444 | SQL injection vulnerability in onethink v.1.1 allows a remote attacker to escalate privileges via a crafted script to the ModelModel.class.php component. | 9.8 | More Details |
| CVE-2024-31705 | An issue in Infotel Conseil GLPI v.10.X.X and after allows a remote attacker to execute arbitrary code via the insufficient validation of user-supplied input. | 9.8 | More Details |
| CVE-2024-33344 | D-Link DIR-822+ V1.0.5 was found to contain a command injection in ftext function of upload_firmware.cgi, which allows remote attackers to execute arbitrary commands via shell. | 9.8 | More Details |
| CVE-2023-50434 | emdns_resolve_raw in emdns.c in emdns through fbd1eef calls strlen with an input that may not be '\0' terminated, leading to a stack-based buffer over-read. This can be triggered by a remote adversary that can send DNS requests to the emdns server. The impact could vary depending on the system libraries, compiler, and processor architecture. Code before be565c3 is unaffected. | 9.8 | More Details |
| CVE-2024-33273 | SQL injection vulnerability in shipup before v.3.3.0 allows a remote attacker to escalate privileges via the getShopID function. | 9.8 | More Details |
| CVE-2023-49473 | Shenzhen JF6000 Cloud Media Collaboration Processing Platform firmware version V1.2.0 and software version V2.0.0 build 6245 is vulnerable to Incorrect Access Control. | 9.8 | More Details |
| CVE-2023-51425 | Improper Privilege Management vulnerability in Jacques Malgrange Rencontre – Dating Site allows Privilege Escalation.This issue affects Rencontre – Dating Site: from n/a through 3.10.1. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-51472 | Improper Authentication vulnerability in Mestres do WP Checkout Mestres WP allows Privilege Escalation.This issue affects Checkout Mestres WP: from n/a through 7.1.9.7. | 9.8 | More Details |
| CVE-2023-51477 | Improper Authentication vulnerability in BUDDYBOSS DMCC BuddyBoss Theme allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects BuddyBoss Theme: from n/a through 2.4.60. | 9.8 | More Details |
| CVE-2023-51478 | Improper Authentication vulnerability in Abdul Hakeem Build App Online allows Privilege Escalation.This issue affects Build App Online: from n/a through 1.0.19. | 9.8 | More Details |
| CVE-2023-51484 | Improper Authentication vulnerability in wp-buy Login as User or Customer (User Switching) allows Privilege Escalation.This issue affects Login as User or Customer (User Switching): from n/a through 3.8. | 9.8 | More Details |
| CVE-2024-31615 | ThinkCMF 6.0.9 is vulnerable to File upload via UeditorController.php. | 9.8 | More Details |
| CVE-2024-33275 | SQL injection vulnerability in Webbax supernewsletter v.1.4.21 and before allows a remote attacker to escalate privileges via the Super Newsletter module in the product_search.php components. | 9.8 | More Details |
| CVE-2024-33269 | SQL Injection vulnerability in Prestaddons flashsales 1.9.7 and before allows an attacker to run arbitrary SQL commands via the FsModel::getFlashSales method. | 9.8 | More Details |
| CVE-2024-34048 | O-RAN RIC I-Release e2mgr lacks array size checks in E2nodeConfigUpdateNotificationHandler. | 9.8 | More Details |
| CVE-2024-0740 | Eclipse Target Management: Terminal and Remote System Explorer (RSE) version <= 4.5.400 has a remote code execution vulnerability that does not require authentication. The fixed version is included in Eclipse IDE 2024-03 | 9.8 | More Details |
| CVE-2024-33267 | SQL Injection vulnerability in Hero hfheropayment v.1.2.5 and before allows an attacker to escalate privileges via the HfHeropaymentGatewayBackModuleFrontController::initContent() function. | 9.8 | More Details |
| CVE-2024-3962 | The Product Addons & Fields for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ppom_upload_file function in all versions up to, and including, 32.0.18. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Successful exploitation requires the PPOM Pro plugin to be installed along with a WooCommerce product that contains a file upload field to retrieve the correct nonce. | 9.8 | More Details |
| CVE-2024-22633 | Setor Informatica Sistema Inteligente para Laboratorios (S.I.L.) 388 was discovered to contain a remote code execution (RCE) vulnerability via the hprinter parameter. This vulnerability is triggered via a crafted POST request. | 9.8 | More Details |
| CVE-2024-33546 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team WZone allows SQL Injection.This issue affects WZone: from n/a through 14.0.10. | 9.6 | More Details |
| CVE-2023-47222 | An exposure of sensitive information vulnerability has been reported to affect Media Streaming add-on. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following version: Media Streaming add-on 500.1.1.5 ( 2024/01/22 ) and later | 9.6 | More Details |
| CVE-2024-30560 | Cross-Site Request Forgery (CSRF) vulnerability in 大侠WP DX-Watermark.This issue affects DX-Watermark: from n/a through 1.0.4. | 9.6 | More Details |
| CVE-2024-3375 | Incorrect Permission Assignment for Critical Resource vulnerability in Havelsan Inc. Dialogue allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Dialogue: from v1.83 before v1.83.1 or v1.84. | 9.4 | More Details |
| CVE-2024-1874 | In PHP versions 8.1.* before 8.1.28, 8.2.* before 8.2.18, 8.3.* before 8.3.5, when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. | 9.4 | More Details |
| CVE-2024-33559 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in 8theme XStore allows SQL Injection.This issue affects XStore: from n/a through 9.3.5. | 9.3 | More Details |
| CVE-2024-32709 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Plechev Andrey WP-Recall.This issue affects WP-Recall: from n/a through 16.26.5. | 9.3 | More Details |
| CVE-2024-33544 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team WZone allows SQL Injection.This issue affects WZone: from n/a through 14.0.10. | 9.3 | More Details |
| CVE-2024-33551 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in 8theme XStore Core allows SQL Injection.This issue affects XStore Core: from n/a through 5.3.5. | 9.3 | More Details |
| CVE-2024-33308 | An issue in TVS Motor Company Limited TVS Connet Android v.4.5.1 and iOS v.5.0.0 allows a remote attacker to escalate privileges via the Emergency Contact Feature. NOTE: this is disputed as discussed in the msn-official/CVE-Evidence repository. | 9.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2019-19755 | ethOS through 1.3.3 ships with SSH host keys baked into the installation image, which allows man-in-the-middle attacks and makes identification of all public IPv4 nodes trivial with Shodan.io. NOTE: as of 2019-12-01, the vendor indicated that they plan to fix this. | 9.1 | More Details |
| CVE-2019-19753 | SimpleMiningOS through v1259 ships with SSH host keys baked into the installation image, which allows man-in-the-middle attacks and makes identification of all public IPv4 nodes trivial with Shodan.io. NOTE: the vendor indicated that they have no plans to fix this, and discourage deployment using public IPv4. | 9.1 | More Details |
| CVE-2024-32948 | Missing Authorization vulnerability in Repute Infosystems ARMember.This issue affects ARMember: from n/a through 4.0.28. | 9.1 | More Details |
| CVE-2024-25343 | Tenda N300 F3 router vulnerability allows users to bypass intended security policy and create weak passwords. | 9.1 | More Details |
| CVE-2024-32880 | pyload is an open-source Download Manager written in pure Python. An authenticated user can change the download folder and upload a crafted template to the specified folder lead to remote code execution. There is no fix available at the time of publication. | 9.1 | More Details |
| CVE-2024-33668 | An issue was discovered in Zammad before 6.3.0. The Zammad Upload Cache uses insecure, partially guessable FormIDs to identify content. An attacker could try to brute force them to upload malicious content to article drafts they have no access to. | 9.1 | More Details |
| CVE-2024-33661 | Portainer before 2.20.0 allows redirects when the target is not index.yaml. | 9.1 | More Details |
| CVE-2022-36029 | Greenlight is an end-user interface for BigBlueButton servers. Versions prior to 2.13.0 have an open redirect vulnerability in the Login page due to unchecked the value of the `return_to` cookie. Versions 2.13.0 contains a patch for the issue. | 9.1 | More Details |
| CVE-2022-36028 | Greenlight is an end-user interface for BigBlueButton servers. Versions prior to 2.13.0 have an open redirect vulnerability in the Login page due to unchecked the value of the `return_to` cookie. Versions 2.13.0 contains a patch for the issue. | 9.1 | More Details |
| CVE-2024-31266 | Improper Control of Generation of Code ('Code Injection') vulnerability in AlgolPlus Advanced Order Export For WooCommerce allows Code Injection.This issue affects Advanced Order Export For WooCommerce: from n/a through 3.4.4. | 9.1 | More Details |
| CVE-2024-32954 | Unrestricted Upload of File with Dangerous Type vulnerability in Tribulant Newsletters.This issue affects Newsletters: from n/a through 4.9.5. | 9.1 | More Details |
| CVE-2024-32836 | Unrestricted Upload of File with Dangerous Type vulnerability in WP Lab WP-Lister Lite for eBay.This issue affects WP-Lister Lite for eBay: from n/a through 3.5.11. | 9.1 | More Details |
| CVE-2024-3411 | Implementations of IPMI Authenticated sessions does not provide enough randomness to protect from session hijacking, allowing an attacker to use either predictable IPMI Session ID or weak BMC Random Number to bypass security controls using spoofed IPMI packets to manage BMC device. | 9.1 | More Details |
| CVE-2024-33553 | Deserialization of Untrusted Data vulnerability in 8theme XStore Core.This issue affects XStore Core: from n/a through 5.3.5. | 9.0 | More Details |
| CVE-2024-22144 | Improper Control of Generation of Code ('Code Injection') vulnerability in Eli Scheetz Anti-Malware Security and Brute-Force Firewall gotmls allows Code Injection.This issue affects Anti-Malware Security and Brute-Force Firewall: from n/a through 4.21.96. | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-6116 | Team ENVY, a Security Research TEAM has found a flaw that allows for a remote code execution on the camera. An attacker could inject malicious into http request packets to execute arbitrary code. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. | 8.9 | More Details |
| CVE-2023-6095 | Vladimir Kononovich, a Security Researcher has found a flaw that allows for a remote code execution on the DVR. An attacker could inject malicious HTTP headers into request packets to execute arbitrary code. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. | 8.9 | More Details |
| CVE-2024-4167 | A vulnerability was found in Tenda 4G300 1.01.42 and classified as critical. Affected by this issue is the function sub_422AA4. The manipulation of the argument year/month/day/hour/minute/second leads to stack-based buffer overflow. The attack may be launched remotely. VDB-261986 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4122 | A vulnerability classified as critical was found in Tenda W15E 15.11.0.14. Affected by this vulnerability is the function formSetDebugCfg of the file /goform/setDebugCfg. The manipulation of the argument enable/level/module leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261865 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4120 | A vulnerability was found in Tenda W15E 15.11.0.14. It has been rated as critical. This issue affects the function formIPMacBindModify of the file /goform/modifyIpMacBind. The manipulation of the argument IPMacBindRuleId/IPMacBindRuleIp/IPMacBindRuleMac/IPMacBindRuleRemark leads to stack-based buffer overflow. 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-261863. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4119 | A vulnerability was found in Tenda W15E 15.11.0.14. It has been declared as critical. This vulnerability affects the function formIPMacBindDel of the file /goform/delIpMacBind. The manipulation of the argument IPMacBindIndex leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-261862 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4118 | A vulnerability was found in Tenda W15E 15.11.0.14. It has been classified as critical. This affects the function formIPMacBindAdd of the file /goform/addIpMacBind. The manipulation of the argument IPMacBindRule leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261861 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-3193 | A vulnerability has been found in MailCleaner up to 2023.03.14 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Admin Endpoints. The manipulation leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier VDB-262309 was assigned to this vulnerability. | 8.8 | More Details |
| CVE-2024-4252 | A vulnerability classified as critical has been found in Tenda i22 1.0.0.3(4687). This affects the function formSetUrlFilterRule. The manipulation of the argument groupIndex leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-262143. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4117 | A vulnerability was found in Tenda W15E 15.11.0.14 and classified as critical. Affected by this issue is the function formDelPortMapping of the file /goform/DelPortMapping. The manipulation of the argument portMappingIndex leads to stack-based buffer overflow. 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-261860. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4116 | A vulnerability has been found in Tenda W15E 15.11.0.14 and classified as critical. Affected by this vulnerability is the function formDelDhcpRule of the file /goform/DelDhcpRule. The manipulation of the argument delDhcpIndex leads to stack-based buffer overflow. 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-261859. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4115 | A vulnerability, which was classified as critical, was found in Tenda W15E 15.11.0.14. Affected is the function formAddDnsForward of the file /goform/AddDnsForward. The manipulation of the argument DnsForwardRule leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-261858 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4251 | A vulnerability was found in Tenda i21 1.0.0.14(4656). It has been rated as critical. Affected by this issue is the function fromDhcpSetSer of the file /goform/DhcpSetSe. The manipulation of the argument dhcpStartIp/dhcpEndIp/dhcpGw/dhcpMask/dhcpLeaseTime/dhcpDns1/dhcpDns2 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-262142 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4250 | A vulnerability was found in Tenda i21 1.0.0.14(4656). It has been declared as critical. Affected by this vulnerability is the function formwrlSSIDset of the file /goform/wifiSSIDset. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-262141 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4249 | A vulnerability was found in Tenda i21 1.0.0.14(4656). It has been classified as critical. Affected is the function formwrlSSIDget of the file /goform/wifiSSIDget. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-262140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4114 | A vulnerability, which was classified as critical, has been found in Tenda TX9 22.03.02.10. This issue affects the function sub_42C014 of the file /goform/PowerSaveSet. The manipulation of the argument time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261857 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4113 | A vulnerability classified as critical was found in Tenda TX9 22.03.02.10. This vulnerability affects the function sub_42D4DC of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. 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-261856. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4112 | A vulnerability classified as critical has been found in Tenda TX9 22.03.02.10. This affects the function sub_42CB94 of the file /goform/SetVirtualServerCfg. The manipulation of the argument list leads to stack-based buffer overflow. 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-261855. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4248 | A vulnerability was found in Tenda i21 1.0.0.14(4656) and classified as critical. This issue affects the function formQosManage_user. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-262139. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4247 | A vulnerability has been found in Tenda i21 1.0.0.14(4656) and classified as critical. This vulnerability affects the function formQosManage_auto. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack can be initiated remotely. VDB-262138 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4246 | A vulnerability, which was classified as critical, was found in Tenda i21 1.0.0.14(4656). This affects the function formQosManageDouble_auto. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The identifier VDB-262137 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4111 | A vulnerability was found in Tenda TX9 22.03.02.10. It has been rated as critical. Affected by this issue is the function sub_42BD7C of the file /goform/SetLEDCfg. The manipulation of the argument time leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-261854 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4245 | A vulnerability, which was classified as critical, has been found in Tenda i21 1.0.0.14(4656). Affected by this issue is the function formQosManageDouble_user. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack may be launched remotely. The identifier of this vulnerability is VDB-262136. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4244 | A vulnerability classified as critical was found in Tenda W9 1.0.0.7(4456). Affected by this vulnerability is the function fromDhcpSetSer of the file /goform/DhcpSetSer. The manipulation of the argument dhcpStartIp/dhcpEndIp/dhcpGw/dhcpMask/dhcpLeaseTime/dhcpDns1/dhcpDns2 leads to stack-based buffer overflow. 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-262135. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4243 | A vulnerability classified as critical has been found in Tenda W9 1.0.0.7(4456). Affected is the function formwrlSSIDset of the file /goform/wifiSSIDset. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-262134 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4121 | A vulnerability classified as critical has been found in Tenda W15E 15.11.0.14. Affected is the function formQOSRuleDel. The manipulation of the argument qosIndex leads to stack-based buffer overflow. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-261864. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4123 | A vulnerability, which was classified as critical, has been found in Tenda W15E 15.11.0.14. Affected by this issue is the function formSetPortMapping of the file /goform/SetPortMapping. The manipulation of the argument portMappingServer/portMappingProtocol/portMappingWan/porMappingtInternal/portMappingExternal leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-261866 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4241 | A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been declared as critical. This vulnerability affects the function formQosManageDouble_auto. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack can be initiated remotely. The identifier of this vulnerability is VDB-262132. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4165 | A vulnerability, which was classified as critical, was found in Tenda G3 15.11.0.17(9502). Affected is the function modifyDhcpRule of the file /goform/modifyDhcpRule. The manipulation of the argument bindDhcpIndex leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-261984. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4303 | ArmorX Android APP's multi-factor authentication (MFA) for the login function is not properly implemented. Remote attackers who obtain user credentials can bypass MFA, allowing them to successfully log into the APP. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3622 | A flaw was found when using mirror-registry to install Quay. It uses a default secret, which is stored in plain-text format in one of the configuration template files. This issue may lead to all instances of Quay deployed using mirror-registry to have the same secret key. This flaw allows a malicious actor to craft session cookies and as a consequence, it may lead to gaining access to the affected Quay instance. | 8.8 | More Details |
| CVE-2024-27322 | Deserialization of untrusted data can occur in the R statistical programming language, on any version starting at 1.4.0 up to and not including 4.4.0, enabling a maliciously crafted RDS (R Data Serialization) formatted file or R package to run arbitrary code on an end user's system when interacted with. | 8.8 | More Details |
| CVE-2024-4171 | A vulnerability classified as critical has been found in Tenda W30E 1.0/1.0.1.25. Affected is the function fromWizardHandle of the file /goform/WizardHandle. The manipulation of the argument PPW leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-261990 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4170 | A vulnerability was found in Tenda 4G300 1.01.42. It has been rated as critical. This issue affects the function sub_429A30. The manipulation of the argument list1 leads to stack-based buffer overflow. The attack may be initiated remotely. The identifier VDB-261989 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4169 | A vulnerability was found in Tenda 4G300 1.01.42. It has been declared as critical. This vulnerability affects the function sub_42775C/sub_4279CC. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be initiated remotely. The identifier of this vulnerability is VDB-261988. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4168 | A vulnerability was found in Tenda 4G300 1.01.42. It has been classified as critical. This affects the function sub_4260F0. The manipulation of the argument upfilen leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-261987. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4301 | N-Reporter and N-Cloud, products of the N-Partner, have an OS Command Injection vulnerability. Remote attackers with normal user privilege can execute arbitrary system commands by manipulating user inputs on a specific page. | 8.8 | More Details |
| CVE-2024-4166 | A vulnerability has been found in Tenda 4G300 1.01.42 and classified as critical. Affected by this vulnerability is the function sub_41E858. The manipulation of the argument GO/page leads to stack-based buffer overflow. The attack can be launched remotely. The identifier VDB-261985 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4164 | A vulnerability, which was classified as critical, has been found in Tenda G3 15.11.0.17(9502). This issue affects the function formModifyPppAuthWhiteMac of the file /goform/ModifyPppAuthWhiteMac. The manipulation of the argument pppoeServerWhiteMacIndex leads to stack-based buffer overflow. 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-261983. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4124 | A vulnerability, which was classified as critical, was found in Tenda W15E 15.11.0.14. This affects the function formSetRemoteWebManage of the file /goform/SetRemoteWebManage. The manipulation of the argument remoteIP leads to stack-based buffer overflow. 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-261867. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-32493 | An issue was discovered in Znuny LTS 6.5.1 through 6.5.7 and Znuny 7.0.1 through 7.0.16 where a logged-in agent is able to inject SQL in the draft form ID parameter of an AJAX request. | 8.8 | More Details |
| CVE-2024-33891 | Delinea Secret Server before 11.7.000001 allows attackers to bypass authentication via the SOAP API in SecretServer/webservices/SSWebService.asmx. This is related to a hardcoded key, the use of the integer 2 for the Admin user, and removal of the oauthExpirationId attribute. | 8.8 | More Details |
| CVE-2024-25917 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in CodeRevolution WP Setup Wizard.This issue affects WP Setup Wizard: from n/a through 1.0.8.1. | 8.8 | More Details |
| CVE-2024-31823 | An issue in Ecommerce-CodeIgniter-Bootstrap commit v. d22b54e8915f167a135046ceb857caaf8479c4da allows a remote attacker to execute arbitrary code via the removeSecondaryImage method of the Publish.php component. | 8.8 | More Details |
| CVE-2024-0840 | The Grandstream UCM Series IP PBX before firmware version 1.0.20.52 is affected by a parameter injection vulnerability in the HTTP interface. A remote and authenticated attacker can execute arbitrary code by sending a crafted HTTP request. Authentication may be possible using a default user and password. Affected models are the UCM6202, UCM6204, UCM6208, and UCM6510. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4127 | A vulnerability was found in Tenda W15E 15.11.0.14. It has been classified as critical. Affected is the function guestWifiRuleRefresh. The manipulation of the argument qosGuestDownstream leads to stack-based buffer overflow. It is possible to launch the attack remotely. VDB-261870 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4126 | A vulnerability was found in Tenda W15E 15.11.0.14 and classified as critical. This issue affects the function formSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument manualTime leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261869 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-20295 | A vulnerability in the CLI of the Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have read-only or higher privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. | 8.8 | More Details |
| CVE-2024-4125 | A vulnerability has been found in Tenda W15E 15.11.0.14 and classified as critical. This vulnerability affects the function formSetStaticRoute of the file /goform/setStaticRoute. The manipulation of the argument staticRouteIndex leads to stack-based buffer overflow. 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-261868. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4242 | A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been rated as critical. This issue affects the function formwrlSSIDget of the file /goform/wifiSSIDget. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-262133 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4291 | A vulnerability was found in Tenda A301 15.13.08.12_multi_TDE01. It has been rated as critical. This issue affects the function formAddMacfilterRule of the file /goform/setBlackRule. The manipulation of the argument deviceList leads to stack-based buffer overflow. 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-262223. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4239 | A vulnerability was found in Tenda AX1806 1.0.0.1 and classified as critical. Affected by this issue is the function formSetRebootTimer of the file /goform/SetRebootTimer. The manipulation of the argument rebootTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-262130 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4237 | A vulnerability, which was classified as critical, was found in Tenda AX1806 1.0.0.1. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-262128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-25575 | A type confusion vulnerability vulnerability exists in the way Foxit Reader 2024.1.0.23997 handles a Lock object. A specially crafted Javascript code inside a malicious PDF document can trigger this vulnerability, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. | 8.8 | More Details |
| CVE-2024-4238 | A vulnerability has been found in Tenda AX1806 1.0.0.1 and classified as critical. Affected by this vulnerability is the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-262129 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-4236 | A vulnerability, which was classified as critical, has been found in Tenda AX1803 1.0.0.1. This issue affects the function formSetSysToolDDNS of the file /goform/SetDDNSCfg. The manipulation of the argument serverName/ddnsUser/ddnsPwd/ddnsDomain leads to stack-based buffer overflow. 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-262127. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-25938 | A use-after-free vulnerability exists in the way Foxit Reader 2024.1.0.23997 handles a Barcode widget. A specially crafted JavaScript code inside a malicious PDF document can trigger reuse of a previously freed object, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. | 8.8 | More Details |
| CVE-2024-23463 | Anti-tampering protection of the Zscaler Client Connector can be bypassed under certain conditions when running the Repair App functionality. This affects Zscaler Client Connector on Windows prior to 4.2.1 | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-28976 | Dell Repository Manager, versions prior to 3.4.5, contains a Path Traversal vulnerability in API module. A local attacker with low privileges could potentially exploit this vulnerability to gain unauthorized write access to the files stored on the server filesystem with the privileges of the running web application. | 8.8 | More Details |
| CVE-2024-33343 | D-Link DIR-822+ V1.0.5 was found to contain a command injection in ChgSambaUserSettings function of prog.cgi, which allows remote attackers to execute arbitrary commands via shell. | 8.8 | More Details |
| CVE-2024-4240 | A vulnerability was found in Tenda W9 1.0.0.7(4456). It has been classified as critical. This affects the function formQosManageDouble_user. The manipulation of the argument ssidIndex leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-262131. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-31406 | Active debug code vulnerability exists in RoamWiFi R10 prior to 4.8.45. If this vulnerability is exploited, a network-adjacent unauthenticated attacker with access to the device may perform unauthorized operations. | 8.8 | More Details |
| CVE-2024-25648 | A use-after-free vulnerability exists in the way Foxit Reader 2024.1.0.23997 handles a ComboBox widget. A specially crafted JavaScript code inside a malicious PDF document can trigger reuse of a previously freed object, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. | 8.8 | More Details |
| CVE-2023-51364 | A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later | 8.7 | More Details |
| CVE-2024-20356 | A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker with Administrator-level privileges to perform command injection attacks on an affected system and elevate their privileges to root. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to elevate their privileges to root. | 8.7 | More Details |
| CVE-2023-51365 | A path traversal vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later | 8.7 | More Details |
| CVE-2024-4161 | In Brocade SANnav, before Brocade SANnav v2.3.0, syslog traffic received clear text. This could allow an unauthenticated, remote attacker to capture sensitive information. | 8.6 | More Details |
| CVE-2024-20353 | A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads. | 8.6 | More Details |
| CVE-2024-33666 | An issue was discovered in Zammad before 6.3.0. Users with customer access to a ticket could have accessed time accounting details of this ticket via the API. This data should be available only to agents. | 8.6 | More Details |
| CVE-2023-46960 | Buffer Overflow vulnerability in PyPXE v.1.8.4 allows a remote attacker to cause a denial of service via the handle function in the tftp module. | 8.6 | More Details |
| CVE-2024-32710 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Plechev Andrey WP-Recall.This issue affects WP-Recall: from n/a through 16.26.5. | 8.5 | More Details |
| CVE-2024-32706 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Repute info systems ARForms.This issue affects ARForms: from n/a through 6.4. | 8.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32876 | NewPipe is an Android app for video streaming written in Java. It supports exporting and importing backups, as a way to let users move their data to a new device effortlessly. However, in versions 0.13.4 through 0.26.1, importing a backup file from an untrusted source could have resulted in Arbitrary Code Execution. This is because backups are serialized/deserialized using Java's Object Serialization Stream Protocol, which can allow constructing any class in the app, unless properly restricted. To exploit this vulnerability, an attacker would need to build a backup file containing the exploit, and then persuade a user into importing it. During the import process, the malicious code would be executed, possibly crashing the app, stealing user data from the NewPipe app, performing nasty actions through Android APIs, and attempting Android JVM/Sandbox escapes through vulnerabilities in the Android OS. The attack can take place only if the user imports a malicious backup file, so an attacker would need to trick a user into importing a backup file from a source they can control. The implementation details of the malicious backup file can be independent of the attacked user or the device they are being run on, and do not require additional privileges. All NewPipe versions from 0.13.4 to 0.26.1 are vulnerable. NewPipe version 0.27.0 fixes the issue by doing the following: Restrict the classes that can be deserialized when calling Java's Object Serialization Stream Protocol, by adding a whitelist with only innocuous data-only classes that can't lead to Arbitrary Code Execution; deprecate backups serialized with Java's Object Serialization Stream Protocol; use JSON serialization for all newly created backups (but still include an alternative file serialized with Java's Object Serialization Stream Protocol in the backup zip for backwards compatibility); show a warning to the user when attempting to import a backup where the only available serialization mode is Java's Object Serialization Stream Protocol (note that in the future this serialization mode will be removed completely). | 8.5 | More Details |
| CVE-2024-2434 | An issue has been discovered in GitLab affecting all versions of GitLab CE/EE 16.9 prior to 16.9.6, 16.10 prior to 16.10.4, and 16.11 prior to 16.11.1 where path traversal could lead to DoS and restricted file read. | 8.5 | More Details |
| CVE-2024-28327 | Asus RT-N12+ B1 router stores user passwords in plaintext, which could allow local attackers to obtain unauthorized access and modify router settings. | 8.4 | More Details |
| CVE-2024-26927 | In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: Add some bounds checking to firmware data Smatch complains about "head->full_size - head->header_size" can underflow. To some extent, we're always going to have to trust the firmware a bit. However, it's easy enough to add a check for negatives, and let's add a upper bounds check as well. | 8.4 | More Details |
| CVE-2024-31837 | DMitry (Deepmagic Information Gathering Tool) 1.3a has a format-string vulnerability, with a threat model similar to CVE-2017-7938. | 8.4 | More Details |
| CVE-2024-25050 | IBM i 7.2, 7.3, 7.4, 7.5 and IBM Rational Development Studio for i 7.2, 7.3, 7.4, 7.5 networking and compiler infrastructure 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 privileges. IBM X-Force ID: 283242. | 8.4 | More Details |
| CVE-2022-48684 | An issue was discovered in Logpoint before 7.1.1. Template injection was seen in the search template. The search template uses jinja templating for generating dynamic data. This could be abused to achieve code execution. Any user with access to create a search template can leverage this to execute code as the loginspect user. | 8.4 | More Details |
| CVE-2024-2663 | The ZD YouTube FLV Player plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.2.6 via the $_GET['image'] parameter. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. | 8.3 | More Details |
| CVE-2023-51471 | Improper Authentication vulnerability in Mestres do WP Checkout Mestres WP allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Checkout Mestres WP: from n/a through 7.1.9.7. | 8.2 | More Details |
| CVE-2024-1969 | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Secomea GateManager (webserver modules) allows crash of GateManager.This issue affects GateManager: from 9.7 before 11.2.624095033. | 8.2 | More Details |
| CVE-2024-22373 | An out-of-bounds write vulnerability exists in the JPEG2000Codec::DecodeByStreamsCommon functionality of Mathieu Malaterre Grassroot DICOM 3.0.23. A specially crafted DICOM file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. | 8.1 | More Details |
| CVE-2024-29320 | Wallos before 1.15.3 is vulnerable to SQL Injection via the category and payment parameters to /subscriptions/get.php. | 8.1 | More Details |
| CVE-2024-4308 | SQL injection vulnerability in HubBank affecting version 1.0.2. This vulnerability could allow an attacker to send a specially crafted SQL query to the database through different endpoints (/admin/view_users.php?id=1,/admin/viewloan-trans.php?id=1,/admin/view-deposit.php?id=1,/admin/view-domtrans.php?id=1, /admin/delete_cards.php?id=1,/admin/view_cards.php?id=1 and /admin/view_users.php?id=1, id parameter) and retrieve the information stored in the database. | 8.1 | More Details |
| CVE-2024-4309 | SQL injection vulnerability in HubBank affecting version 1.0.2. This vulnerability could allow an attacker to send a specially crafted SQL query to the database through different endpoints (/user/transaction.php?id=1, /user/credit-debit_transaction.php?id=1,/user/view_transaction. php?id=1 and /user/viewloantrans.php?id=1, id parameter) and retrieve the information stored in the database. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-1579 | Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) vulnerability in Secomea GateManager (Webserver modules) allows Session Hijacking.This issue affects GateManager: before 11.2.624071020. | 8.1 | More Details |
| CVE-2024-4307 | SQL injection vulnerability in HubBank affecting version 1.0.2. This vulnerability could allow an attacker to send a specially crafted SQL query to the database through different endpoints (/accounts/activities.php?id=1, /accounts/view-deposit.php?id=1, /accounts/view_cards. php?id=1, /accounts/wire-transfer.php?id=1 and /accounts/wiretransfer-pending.php?id=1, id parameter) and retrieve the information stored in the database. | 8.1 | More Details |
| CVE-2024-33531 | cdbattags lua-resty-jwt 0.2.3 allows attackers to bypass all JWT-parsing signature checks by crafting a JWT with an enc header with the value A256GCM. | 8.1 | More Details |
| CVE-2024-3623 | A flaw was found when using mirror-registry to install Quay. It uses a default database secret key, which is stored in plain-text format in one of the configuration template files. This issue may lead to all instances of Quay deployed using mirror-registry to have the same database secret key. This flaw allows a malicious actor to access sensitive information from Quay's database. | 8.1 | More Details |
| CVE-2024-2505 | The GamiPress WordPress plugin before 6.8.9's access control mechanism fails to properly restrict access to its settings, permitting Authors to manipulate requests and extend access to lower privileged users, like Subscribers, despite initial settings prohibiting such access. This vulnerability resembles broken access control, enabling unauthorized users to modify critical GamiPress WordPress plugin before 6.8.9 configurations. | 8.1 | More Details |
| CVE-2024-4185 | The Customer Email Verification for WooCommerce plugin for WordPress is vulnerable to Email Verification and Authentication Bypass in all versions up to, and including, 2.7.4 via the use of insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification, and if both the "Login the user automatically after the account is verified" and "Verify account for current users" options are checked, then it potentially makes it possible for attackers to bypass authentication for other users. | 8.1 | More Details |
| CVE-2024-31502 | An issue in Insurance Management System v.1.0.0 and before allows a remote attacker to escalate privileges via a crafted POST request to /admin/core/new_staff. | 8.1 | More Details |
| CVE-2024-1657 | A flaw was found in the ansible automation platform. An insecure WebSocket connection was being used in installation from the Ansible rulebook EDA server. An attacker that has access to any machine in the CIDR block could download all rulebook data from the WebSocket, resulting in loss of confidentiality and integrity of the system. | 8.1 | More Details |
| CVE-2023-52727 | Open Networking Foundation SD-RAN ONOS onos-lib-go 0.10.25 allows an index out-of-range condition in parseAlignBits. | 8.1 | More Details |
| CVE-2023-46304 | modules/Users/models/Module.php in Vtiger CRM 7.5.0 allows a remote authenticated attacker to run arbitrary PHP code because an unprotected endpoint allows them to write this code to the config.inc.php file (executed on every page load). | 8.1 | More Details |
| CVE-2023-52724 | Open Networking Foundation SD-RAN onos-kpimon 0.4.7 allows out-of-bounds array access in the processIndicationFormat1 function. | 8.1 | More Details |
| CVE-2024-4163 | The Skylab IGX IIoT Gateway allowed users to connect to it via a limited shell terminal (IGX). However, it was discovered that the process was running under root privileges. This allowed the attacker to read, write, and modify any file in the operating system by utilizing the limited shell file exec and download functions. By replacing the /etc/passwd file with a new root user entry, the attacker was able to breakout from the limited shell and login to a unrestricted shell with root access. With the root access, the attacker will be able take full control of the IIoT Gateway. | 8.0 | More Details |
| CVE-2024-33438 | File Upload vulnerability in CubeCart before 6.5.5 allows an authenticated user to execute arbitrary code via a crafted .phar file. | 8.0 | More Details |
| CVE-2024-2378 | A vulnerability exists in the web-authentication component of the SDM600. If exploited an attacker could escalate privileges on affected installations. | 8.0 | More Details |
| CVE-2024-31821 | SQL Injection vulnerability in Ecommerce-CodeIgniter-Bootstrap commit v. d22b54e8915f167a135046ceb857caaf8479c4da allows a remote attacker to execute arbitrary code via the manageQuantitiesAndProcurement method of the Orders_model.php component. | 8.0 | More Details |
| CVE-2022-48611 | A logic issue was addressed with improved checks. This issue is fixed in iTunes 12.12.4 for Windows. A local attacker may be able to elevate their privileges. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4192 | Delta Electronics CNCSoft-G2 lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. | 7.8 | More Details |
| CVE-2022-48662 | In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Really move i915_gem_context.link under ref protection i915_perf assumes that it can use the i915_gem_context reference to protect its i915->gem.contexts.list iteration. However, this requires that we do not remove the context from the list until after we drop the final reference and release the struct. If, as currently, we remove the context from the list during context_close(), the link.next pointer may be poisoned while we are holding the context reference and cause a GPF: [ 4070.573157] i915 0000:00:02.0: [drm:i915_perf_open_ioctl [i915]] filtering on ctx_id=0x1fffff ctx_id_mask=0x1fffff [ 4070.574881] general protection fault, probably for non-canonical address 0xdead000000000100: 0000 [#1] PREEMPT SMP [ 4070.574897] CPU: 1 PID: 284392 Comm: amd_performance Tainted: G E 5.17.9 #180 [ 4070.574903] Hardware name: Intel Corporation NUC7i5BNK/NUC7i5BNB, BIOS BNKBL357.86A.0052.2017.0918.1346 09/18/2017 [ 4070.574907] RIP: 0010:oa_configure_all_contexts.isra.0+0x222/0x350 [i915] [ 4070.574982] Code: 08 e8 32 6e 10 e1 4d 8b 6d 50 b8 ff ff ff ff 49 83 ed 50 f0 41 0f c1 04 24 83 f8 01 0f 84 e3 00 00 00 85 c0 0f 8e fa 00 00 00 <49> 8b 45 50 48 8d 70 b0 49 8d 45 50 48 39 44 24 10 0f 85 34 fe ff [ 4070.574990] RSP: 0018:ffffc90002077b78 EFLAGS: 00010202 [ 4070.574995] RAX: 0000000000000002 RBX: 0000000000000002 RCX: 0000000000000000 [ 4070.575000] RDX: 0000000000000001 RSI: ffffc90002077b20 RDI: ffff88810ddc7c68 [ 4070.575004] RBP: 0000000000000001 R08: ffff888103242648 R09: fffffffffffffffc [ 4070.575008] R10: ffffffff82c50bc0 R11: 0000000000025c80 R12: ffff888101bf1860 [ 4070.575012] R13: dead000000000b0 R14: ffffc90002077c04 R15: ffff88810be5cabc [ 4070.575016] FS: 00007f1ed50c0780(0000) GS:ffff88885ec80000(0000) knlGS:0000000000000000 [ 4070.575021] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [ 4070.575025] CR2: 00007f1ed5590280 CR3: 000000010ef6f005 CR4: 00000000003706e0 [ 4070.575029] Call Trace: [ 4070.575033] <TASK> [ 4070.575037] lrc_configure_all_contexts+0x13e/0x150 [i915] [ 4070.575103] gen8_enable_metric_set+0x4d/0x90 [i915] [ 4070.575164] i915_perf_open_ioctl+0xbc0/0x1500 [i915] [ 4070.575224] ? asm_common_interrupt+0x1e/0x40 [ 4070.575232] ? i915_oa_init_reg_state+0x110/0x110 [i915] [ 4070.575290] drm_ioctl_kernel+0x85/0x110 [ 4070.575296] ? update_load_avg+0x5f/0x5e0 [ 4070.575302] drm_ioctl+0x1d3/0x370 [ 4070.575307] ? i915_oa_init_reg_state+0x110/0x110 [i915] [ 4070.575382] ? gen8_gt_irq_handler+0x46/0x130 [i915] [ 4070.575445] __x64_sys_ioctl+0x3c4/0x8d0 [ 4070.575451] ? __do_softirq+0xaa/0x1d2 [ 4070.575456] do_syscall_64+0x35/0x80 [ 4070.575461] entry_SYSCALL_64_after_hwframe+0x44/0xae [ 4070.575467] RIP: 0033:0x7f1ed5c10397 [ 4070.575471] Code: 3c 1c e8 1c ff ff ff 85 c0 79 87 49 c7 c4 ff ff ff ff 5b 5d 4c 89 e0 41 5c c3 66 0f 1f 84 00 00 00 00 00 b8 10 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d a9 da 0d 00 f7 d8 64 89 01 48 [ 4070.575478] RSP: 002b:00007ffd65c8d7a8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [ 4070.575484] RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f1ed5c10397 [ 4070.575488] RDX: 00007ffd65c8d7c0 RSI: 0000000040106476 RDI: 0000000000000006 [ 4070.575492] RBP: 00005620972f9c60 R08: 000000000000000a R09: 0000000000000005 [ 4070.575496] R10: 000000000000000d R11: 0000000000000246 R12: 000000000000000a [ 4070.575500] R13: 000000000000000d R14: 0000000000000000 R15: 00007ffd65c8d7c0 [ 4070.575505] </TASK> [ 4070.575507] Modules linked in: nls_ascii(E) nls_cp437(E) vfat(E) fat(E) i915(E) x86_pkg_temp_thermal(E) intel_powerclamp(E) crct10dif_pclmul(E) crc32_pclmul(E) crc32c_intel(E) aesni_intel(E) crypto_simd(E) intel_gtt(E) cryptd(E) ttm(E) rapl(E) intel_cstate(E) drm_kms_helper(E) cfbfillrect(E) syscopyarea(E) cfbimgblt(E) intel_uncore(E) sysfillrect(E) mei_me(E) sysimgblt(E) i2c_i801(E) fb_sys_fops(E) mei(E) intel_pch_thermal(E) i2c_smbus ---truncated--- | 7.8 | More Details |
| CVE-2022-48658 | In the Linux kernel, the following vulnerability has been resolved: mm: slub: fix flush_cpu_slab()/__free_slab() invocations in task context. Commit 5a836bf6b09f ("mm: slub: move flush_cpu_slab() invocations __free_slab() invocations out of IRQ context") moved all flush_cpu_slab() invocations to the global workqueue to avoid a problem related with deactivate_slab()/__free_slab() being called from an IRQ context on PREEMPT_RT kernels. When the flush_all_cpu_locked() function is called from a task context it may happen that a workqueue with WQ_MEM_RECLAIM bit set ends up flushing the global workqueue, this will cause a dependency issue. workqueue: WQ_MEM_RECLAIM nvme-delete-wq:nvme_delete_ctrl_work [nvme_core] is flushing !WQ_MEM_RECLAIM events:flush_cpu_slab WARNING: CPU: 37 PID: 410 at kernel/workqueue.c:2637 check_flush_dependency+0x10a/0x120 Workqueue: nvme-delete-wq nvme_delete_ctrl_work [nvme_core] RIP: 0010:check_flush_dependency+0x10a/0x120[ 453.262125] Call Trace: __flush_work.isra.0+0xbf/0x220 ? __queue_work+0x1dc/0x420 flush_all_cpus_locked+0xfb/0x120 __kmem_cache_shutdown+0x2b/0x320 kmem_cache_destroy+0x49/0x100 bioset_exit+0x143/0x190 blk_release_queue+0xb9/0x100 kobject_cleanup+0x37/0x130 nvme_fc_ctrl_free+0xc6/0x150 [nvme_fc] nvme_free_ctrl+0x1ac/0x2b0 [nvme_core] Fix this bug by creating a workqueue for the flush operation with the WQ_MEM_RECLAIM bit set. | 7.8 | More Details |
| CVE-2023-51794 | Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/af_stereowiden.c:120:69. | 7.8 | More Details |
| CVE-2022-48657 | In the Linux kernel, the following vulnerability has been resolved: arm64: topology: fix possible overflow in amu_fie_setup() cpufreq_get_hw_max_freq() returns max frequency in kHz as *unsigned int*, while freq_inv_set_max_ratio() gets passed this frequency in Hz as 'u64'. Multiplying max frequency by 1000 can potentially result in overflow -- multiplying by 1000ULL instead should avoid that... Found by Linux Verification Center (linuxtesting.org) with the SVACE static analysis tool. | 7.8 | More Details |
| CVE-2024-27518 | An issue in SUPERAntiSyware Professional X 10.0.1262 and 10.0.1264 allows unprivileged attackers to escalate privileges via a restore of a crafted DLL file into the C:\Program Files\SUPERAntiSpyware folder. | 7.8 | More Details |
| CVE-2024-23773 | An issue was discovered in Quest KACE Agent for Windows 12.0.38 and 13.1.23.0. An Arbitrary file delete vulnerability exists in the KSchedulerSvc.exe component. Local attackers can delete any file of their choice with NT Authority\SYSTEM privileges. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48655 | In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Harden accesses to the reset domains Accessing reset domains descriptors by the index upon the SCMI drivers requests through the SCMI reset operations interface can potentially lead to out-of-bound violations if the SCMI driver misbehave. Add an internal consistency check before any such domains descriptors accesses. | 7.8 | More Details |
| CVE-2024-32324 | Buffer Overflow vulnerability in Shenzhen Libituo Technology Co., Ltd LBT-T300-T400 v.3.2 allows a local attacker to execute arbitrary code via the vpn_client_ip variable of the config_vpn_pptp function in rc program. | 7.8 | More Details |
| CVE-2024-33673 | An issue was discovered in Veritas Backup Exec before 22.2 HotFix 917391. Improper access controls allow for DLL Hijacking in the Windows DLL Search path. | 7.8 | More Details |
| CVE-2024-23774 | An issue was discovered in Quest KACE Agent for Windows 12.0.38 and 13.1.23.0. An unquoted Windows search path vulnerability exists in the KSchedulerSvc.exe and AMPTools.exe components. This allows local attackers to execute code of their choice with NT Authority\SYSTEM privileges. | 7.8 | More Details |
| CVE-2023-52080 | IEIT NF5280M6 UEFI firmware through 8.4 has a pool overflow vulnerability, caused by improper use of the gRT->GetVariable() function. Attackers with access to local NVRAM variables can exploit this by modifying these variables on SPI Flash, resulting in memory data being tampered with. When critical data in memory data is tampered with,a crash may occur. | 7.7 | More Details |
| CVE-2024-33671 | An issue was discovered in Veritas Backup Exec before 22.2 HotFix 917391. The Backup Exec Deduplication Multi-threaded Streaming Agent can be leveraged to perform arbitrary file deletion on protected files. | 7.7 | More Details |
| CVE-2024-22391 | A heap-based buffer overflow vulnerability exists in the LookupTable::SetLUT functionality of Mathieu Malaterre Grassroot DICOM 3.0.23. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability. | 7.7 | More Details |
| CVE-2022-48685 | An issue was discovered in Logpoint 7.1 before 7.1.2. The daily executed cron file clean_secbi_old_logs is writable by all users and is executed as root, leading to privilege escalation. | 7.7 | More Details |
| CVE-2024-1139 | A credentials leak vulnerability was found in the cluster monitoring operator in OCP. This issue may allow a remote attacker who has basic login credentials to check the pod manifest to discover a repository pull secret. | 7.7 | More Details |
| CVE-2022-48651 | In the Linux kernel, the following vulnerability has been resolved: ipvlan: Fix out-of-bound bugs caused by unset skb->mac_header If an AF_PACKET socket is used to send packets through ipvlan and the default xmit function of the AF_PACKET socket is changed from dev_queue_xmit() to packet_direct_xmit() via setsockopt() with the option name of PACKET_QDISC_BYPASS, the skb->mac_header may not be reset and remains as the initial value of 65535, this may trigger slab-out-of-bounds bugs as following: ================================================================== UG: KASAN: slab-out-of-bounds in ipvlan_xmit_mode_l2+0xdb/0x330 [ipvlan] PU: 2 PID: 1768 Comm: raw_send Kdump: loaded Not tainted 6.0.0-rc4+ #6 ardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-1.fc33 all Trace: print_address_description.constprop.0+0x1d/0x160 print_report.cold+0x4f/0x112 kasan_report+0xa3/0x130 ipvlan_xmit_mode_l2+0xdb/0x330 [ipvlan] ipvlan_start_xmit+0x29/0xa0 [ipvlan] __dev_direct_xmit+0x2e2/0x380 packet_direct_xmit+0x22/0x60 packet_snd+0x7c9/0xc40 sock_sendmsg+0x9a/0xa0 __sys_sendto+0x18a/0x230 __x64_sys_sendto+0x74/0x90 do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd The root cause is: 1. packet_snd() only reset skb->mac_header when sock->type is SOCK_RAW and skb->protocol is not specified as in packet_parse_headers() 2. packet_direct_xmit() doesn't reset skb->mac_header as dev_queue_xmit() In this case, skb->mac_header is 65535 when ipvlan_xmit_mode_l2() is called. So when ipvlan_xmit_mode_l2() gets mac header with eth_hdr() which use "skb->head + skb->mac_header", out-of-bound access occurs. This patch replaces eth_hdr() with skb_eth_hdr() in ipvlan_xmit_mode_l2() and reset mac header in multicast to solve this out-of-bound bug. | 7.7 | More Details |
| CVE-2024-33672 | An issue was discovered in Veritas NetBackup before 10.4. The Multi-Threaded Agent used in NetBackup can be leveraged to perform arbitrary file deletion on protected files. | 7.7 | More Details |
| CVE-2024-32883 | MCUboot is a secure bootloader for 32-bits microcontrollers. MCUboot uses a TLV (tag-length-value) structure to represent the meta data associated with an image. The TLVs themselves are divided into two sections, a protected and an unprotected section. The protected TLV entries are included as part of the image signature to avoid tampering. However, the code does not distinguish which TLV entries should be protected or not, so it is possible for an attacker to add unprotected TLV entries that should be protected. Currently, the primary protected TLV entries should be the dependency indication, and the boot record. An injected dependency value would primarily result in an otherwise acceptable image being rejected. A boot record injection could allow fields in a later attestation record to include data not intended, which could cause an image to appear to have properties that it should not have. As a workaround, disable the boot record functionality. | 7.7 | More Details |
| CVE-2024-2377 | A vulnerability exists in the too permissive HTTP response header web server settings of the SDM600. An attacker can take advantage of this and possibly carry out privileged actions and access sensitive information. | 7.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-31621 | An issue in FlowiseAI Inc Flowise v.1.6.2 and before allows a remote attacker to execute arbitrary code via a crafted script to the api/v1 component. | 7.6 | More Details |
| CVE-2024-28320 | Insecure Direct Object References (IDOR) vulnerability in Hospital Management System 1.0 allows attackers to manipulate user parameters for unauthorized access and modifications via crafted POST request to /patient/edit-user.php. | 7.6 | More Details |
| CVE-2024-4173 | A vulnerability in Brocade SANnav exposes Kafka in the wan interface. The vulnerability could allow an unauthenticated attacker to perform various attacks, including DOS against the Brocade SANnav. | 7.6 | More Details |
| CVE-2024-31755 | cJSON v1.7.17 was discovered to contain a segmentation violation, which can trigger through the second parameter of function cJSON_SetValuestring at cJSON.c. | 7.6 | More Details |
| CVE-2023-50053 | An issue in Foundation.app Foundation platform 1.0 allows a remote attacker to obtain sensitive information via the Web3 authentication process of Foundation, the signed message lacks a nonce (random number) | 7.6 | More Details |
| CVE-2024-4337 | Adive Framework 2.0.8, does not sufficiently encode user-controlled inputs, resulting in a persistent Cross-Site Scripting (XSS) vulnerability via the /adive/admin/nav/add, in multiple parameters. This vulnerability allows an attacker to retrieve the session details of an authenticated user. | 7.6 | More Details |
| CVE-2024-4336 | Adive Framework 2.0.8, does not sufficiently encode user-controlled inputs, resulting in a persistent Cross-Site Scripting (XSS) vulnerability via the /adive/admin/tables/add, in multiple parameters. An attacker could retrieve the session details of an authenticated user. | 7.6 | More Details |
| CVE-2024-4225 | Multiple security vulnerabilities has been discovered in web interface of NetGuardian DIN Remote Telemetry Unit (RTU), by DPS Telecom. Attackers can exploit those security vulnerabilities to perform critical actions such as escalate user's privilege, steal user's credential, Cross Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). | 7.6 | More Details |
| CVE-2024-33597 | Missing Authorization vulnerability in ProFaceOff SSU.This issue affects SSU: from n/a through 1.5.0. | 7.5 | More Details |
| CVE-2024-29384 | An issue in CSS Exfil Protection v.1.1.0 allows a remote attacker to obtain sensitive information via the content.js and parseCSSRules functions. | 7.5 | More Details |
| CVE-2024-33383 | Arbitrary File Read vulnerability in novel-plus 4.3.0 and before allows a remote attacker to obtain sensitive information via a crafted GET request using the filePath parameter. | 7.5 | More Details |
| CVE-2024-33437 | An issue in CSS Exfil Protection v.1.1.0 allows a remote attacker to obtain sensitive information due to missing support for CSS Style Rules. | 7.5 | More Details |
| CVE-2024-32406 | Server-Side Template Injection (SSTI) vulnerability in inducer relate before v.2024.1 allows a remote attacker to execute arbitrary code via a crafted payload to the Batch-Issue Exam Tickets function. | 7.5 | More Details |
| CVE-2024-33635 | Missing Authorization vulnerability in Piotnet Piotnet Addons For Elementor Pro.This issue affects Piotnet Addons For Elementor Pro: from n/a through 7.1.17. | 7.5 | More Details |
| CVE-2024-33591 | Missing Authorization vulnerability in Tips and Tricks HQ Easy Accept Payments.This issue affects Easy Accept Payments: from n/a through 4.9.10. | 7.5 | More Details |
| CVE-2024-34088 | In FRRouting (FRR) through 9.1, it is possible for the get_edge() function in ospf_te.c in the OSPF daemon to return a NULL pointer. In cases where calling functions do not handle the returned NULL value, the OSPF daemon crashes, leading to denial of service. | 7.5 | More Details |
| CVE-2024-27124 | An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later | 7.5 | More Details |
| CVE-2024-33594 | Missing Authorization vulnerability in Leaky Paywall.This issue affects Leaky Paywall: from n/a through 4.20.8. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-33637 | Insertion of Sensitive Information into Log File vulnerability in Solid Plugins Solid Affiliate.This issue affects Solid Affiliate: from n/a through 1.9.1. | 7.5 | More Details |
| CVE-2023-6596 | An incomplete fix was shipped for the Rapid Reset (CVE-2023-44487/CVE-2023-39325) vulnerability for an OpenShift Containers. | 7.5 | More Details |
| CVE-2024-31801 | Directory Traversal vulnerability in NEXSYS-ONE before v.Rev.15320 allows a remote attacker to obtain sensitive information via a crafted request. | 7.5 | More Details |
| CVE-2024-32269 | An issue in Yonganda YAD-LOJ V3.0.561 allows a remote attacker to cause a denial of service via a crafted packet. | 7.5 | More Details |
| CVE-2024-34046 | The O-RAN E2T I-Release Prometheus metric Increment function can crash in sctpThread.cpp for message.peerInfo->sctpParams->e2tCounters[IN_SUCC][MSG_COUNTER][ProcedureCode_id_RICsubscription]->Increment(). | 7.5 | More Details |
| CVE-2024-33274 | Directory Traversal vulnerability in FME Modules customfields v.2.2.7 and before allows a remote attacker to obtain sensitive information via the Custom Checkout Fields, Add Custom Fields to Checkout parameter of the ajax.php | 7.5 | More Details |
| CVE-2024-32825 | Insertion of Sensitive Information into Log File vulnerability in Patrick Posner Simply Static.This issue affects Simply Static: from n/a through 3.1.3. | 7.5 | More Details |
| CVE-2024-33270 | An issue in FME Modules fileuploads v.2.0.3 and before and fixed in v2.0.4 allows a remote attacker to obtain sensitive information via the uploadfiles.php component. | 7.5 | More Details |
| CVE-2024-32953 | Insertion of Sensitive Information into Log File vulnerability in Newsletters.This issue affects Newsletters: from n/a through 4.9.5. | 7.5 | More Details |
| CVE-2024-28716 | An issue in OpenStack Storlets yoga-eom allows a remote attacker to execute arbitrary code via the gateway.py component. | 7.5 | More Details |
| CVE-2024-25048 | IBM MQ Appliance 9.3 CD and LTS are vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash. IBM X-Force ID: 283137. | 7.5 | More Details |
| CVE-2024-34045 | The O-RAN E2T I-Release Prometheus metric Increment function can crash in sctpThread.cpp for message.peerInfo->counters[IN_INITI][MSG_COUNTER][ProcedureCode_id_E2setup]->Increment(). | 7.5 | More Details |
| CVE-2023-47504 | Improper Authentication vulnerability in Elementor Elementor Website Builder allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Elementor Website Builder: from n/a through 3.16.4. | 7.5 | More Details |
| CVE-2024-33309 | An issue in TVS Motor Company Limited TVS Connet Android v.4.5.1 and iOS v.5.0.0 allows a remote attacker to obtain sensitive information via an insecure API endpoint. NOTE: this is disputed as discussed in the msn-official/CVE-Evidence repository. | 7.5 | More Details |
| CVE-2024-34049 | Open Networking Foundation SD-RAN Rimedo rimedo-ts 0.1.1 has a slice bounds out-of-range panic in "return plmnIdString[0:3], plmnIdString[3:]" in reader.go. | 7.5 | More Details |
| CVE-2024-34050 | Open Networking Foundation SD-RAN Rimedo rimedo-ts 0.1.1 has a slice bounds out-of-range panic in "return uint64(b[2])<<16 \| uint64(b[1])<<8 \| uint64(b[0])" in reader.go. | 7.5 | More Details |
| CVE-2024-1895 | The Event Monster – Event Management, Tickets Booking, Upcoming Event plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.3.4 via deserialization via shortcode of untrusted input from a custom meta value. This makes it possible for authenticated attackers, with contributor access 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. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-45385 | ProQuality pqprintshippinglabels before v.4.15.0 is vulnerable to Directory Traversal via the pqprintshippinglabels module. | 7.5 | More Details |
| CVE-2023-23976 | Incorrect Default Permissions vulnerability in Metagauss RegistrationMagic allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects RegistrationMagic: from n/a through 5.1.9.2. | 7.5 | More Details |
| CVE-2024-3052 | Malformed S2 Nonce Get command classes can be sent to crash the gateway. A hard reset is required to recover the gateway. | 7.5 | More Details |
| CVE-2024-3051 | Malformed Device Reset Locally command classes can be sent to temporarily deny service to an end device. Any frames sent by the end device will not be acknowledged by the gateway during this time. | 7.5 | More Details |
| CVE-2024-2757 | In PHP 8.3.* before 8.3.5, function mb_encode_mimeheader() runs endlessly for some inputs that contain long strings of non-space characters followed by a space. This could lead to a potential DoS attack if a hostile user sends data to an application that uses this function. | 7.5 | More Details |
| CVE-2024-32816 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PickPlugins Post Grid.This issue affects Post Grid: from n/a through 2.2.78. | 7.5 | More Details |
| CVE-2024-4340 | Passing a heavily nested list to sqlparse.parse() leads to a Denial of Service due to RecursionError. | 7.5 | More Details |
| CVE-2023-46565 | Buffer Overflow vulnerability in osrg gobgp commit 419c50dfac578daa4d11256904d0dc182f1a9b22 allows a remote attacker to cause a denial of service via the handlingError function in pkg/server/fsm.go. | 7.5 | More Details |
| CVE-2024-2829 | An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.5 before 16.9.6, all versions starting from 16.10 before 16.10.4, all versions starting from 16.11 before 16.11.1. A crafted wildcard filter in FileFinder may lead to a denial of service. | 7.5 | More Details |
| CVE-2024-26331 | ReCrystallize Server 5.10.0.0 uses a authorization mechanism that relies on the value of a cookie, but it does not bind the cookie value to a session ID. Attackers can easily modify the cookie value, within a browser or by implementing client-side code outside of a browser. Attackers can bypass the authentication mechanism by modifying the cookie to contain an expected value. | 7.5 | More Details |
| CVE-2024-25583 | A crafted response from an upstream server the recursor has been configured to forward-recurse to can cause a Denial of Service in the Recursor. The default configuration of the Recursor does not use recursive forwarding and is not affected. | 7.5 | More Details |
| CVE-2024-33342 | D-Link DIR-822+ V1.0.5 was found to contain a command injection in SetPlcNetworkpwd function of prog.cgi, which allows remote attackers to execute arbitrary commands via shell. | 7.5 | More Details |
| CVE-2024-32781 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ThemeHigh Email Customizer for WooCommerce.This issue affects Email Customizer for WooCommerce: from n/a through 2.6.0. | 7.5 | More Details |
| CVE-2024-4056 | Denial of service condition in M-Files Server in versions before 24.4.13592.4 and after 23.11 (excluding 24.2 LTS) allows unauthenticated user to consume computing resources. | 7.5 | More Details |
| CVE-2024-31551 | Directory Traversal vulnerability in lib/admin/image.admin.php in cmseasy v7.7.7.9 20240105 allows attackers to delete arbitrary files via crafted GET request. | 7.5 | More Details |
| CVE-2024-33271 | An issue in FME Modules eventsmanager before 4.4.0 allows an attacker to obtain sensitive information from the ps_customer component. | 7.5 | More Details |
| CVE-2023-46566 | Buffer Overflow vulnerability in msoulier tftpy commit 467017b844bf6e31745138a30e2509145b0c529c allows a remote attacker to cause a denial of service via the parse function in the TftpPacketFactory class. | 7.5 | More Details |
| CVE-2024-32726 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in vinoth06. Frontend Dashboard.This issue affects Frontend Dashboard: from n/a through 2.2.2. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32358 | An issue in Jpress v.5.1.0 allows a remote attacker to execute arbitrary code via a crafted script to the custom plug-in module function, a different vulnerability than CVE-2024-43033. | 7.5 | More Details |
| CVE-2023-6096 | Vladimir Kononovich, a Security Researcher has found a flaw that using a inappropriate encryption logic on the DVR. firmware encryption is broken and allows to decrypt. The manufacturer has released patch firmware for the flaw, please refer to the manufacturer's report for details and workarounds. | 7.4 | More Details |
| CVE-2024-20313 | A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. | 7.4 | More Details |
| CVE-2022-48666 | In the Linux kernel, the following vulnerability has been resolved: scsi: core: Fix a use-after-free There are two .exit_cmd_priv implementations. Both implementations use resources associated with the SCSI host. Make sure that these resources are still available when .exit_cmd_priv is called by waiting inside scsi_remove_host() until the tag set has been freed. This commit fixes the following use-after-free: ================================================================== BUG: KASAN: use-after-free in srp_exit_cmd_priv+0x27/0xd0 [ib_srp] Read of size 8 at addr ffff888100337000 by task multipathd/16727 Call Trace: <TASK> dump_stack_lvl+0x34/0x44 print_report.cold+0x5e/0x5db kasan_report+0xab/0x120 srp_exit_cmd_priv+0x27/0xd0 [ib_srp] scsi_mq_exit_request+0x4d/0x70 blk_mq_free_rqs+0x143/0x410 __blk_mq_free_map_and_rqs+0x6e/0x100 blk_mq_free_tag_set+0x2b/0x160 scsi_host_dev_release+0xf3/0x1a0 device_release+0x54/0xe0 kobject_put+0xa5/0x120 device_release+0x54/0xe0 kobject_put+0xa5/0x120 scsi_device_dev_release_usercontext+0x4c1/0x4e0 execute_in_process_context+0x23/0x90 device_release+0x54/0xe0 kobject_put+0xa5/0x120 scsi_disk_release+0x3f/0x50 device_release+0x54/0xe0 kobject_put+0xa5/0x120 disk_release+0x17f/0x1b0 device_release+0x54/0xe0 kobject_put+0xa5/0x120 dm_put_table_device+0xa3/0x160 [dm_mod] dm_put_device+0xd0/0x140 [dm_mod] free_priority_group+0xd8/0x110 [dm_multipath] free_multipath+0x94/0xe0 [dm_multipath] dm_table_destroy+0xa2/0x1e0 [dm_mod] __dm_destroy+0x196/0x350 [dm_mod] dev_remove+0x10c/0x160 [dm_mod] ctl_ioctl+0x2c2/0x590 [dm_mod] dm_ctl_ioctl+0x5/0x10 [dm_mod] __x64_sys_ioctl+0xb4/0xf0 dm_ctl_ioctl+0x5/0x10 [dm_mod] __x64_sys_ioctl+0xb4/0xf0 do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x46/0xb0 | 7.4 | More Details |
| CVE-2023-50363 | An incorrect authorization vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to bypass intended access restrictions via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later | 7.4 | More Details |
| CVE-2024-33831 | A stored cross-site scripting (XSS) vulnerability in the Advanced Expectation - Response module of yapi v1.10.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the body field. | 7.4 | More Details |
| CVE-2024-3625 | A flaw was found in Quay, where Quay's database is stored in plain text in mirror-registry on Jinja's config.yaml file. This issue leaves the possibility of a malicious actor with access to this file to gain access to Quay's Redis instance. | 7.3 | More Details |
| CVE-2024-3624 | A flaw was found in how Quay's database is stored in plain-text in mirror-registry on the jinja's config.yaml file. This flaw allows a malicious actor with access to this file to gain access to Quay's database. | 7.3 | More Details |
| CVE-2024-4349 | A vulnerability has been found in SourceCodester Pisay Online E-Learning System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /lesson/controller.php. The manipulation of the argument file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-262489 was assigned to this vulnerability. | 7.3 | More Details |
| CVE-2024-33338 | Cross Site Scripting vulnerability in jizhicms v.2.5.4 allows a remote attacker to obtain sensitive information via a crafted article publication request. | 7.3 | More Details |
| CVE-2024-28241 | The GLPI Agent is a generic management agent. Prior to version 1.7.2, a local user can modify GLPI-Agent code or used DLLs to modify agent logic and even gain higher privileges. Users should upgrade to GLPI-Agent 1.7.2 to receive a patch. As a workaround, use the default installation folder which involves installed folder is automatically secured by the system. | 7.3 | More Details |
| CVE-2024-28240 | The GLPI Agent is a generic management agent. A vulnerability that only affects GLPI-Agent installed on windows via MSI packaging can allow a local user to cause denial of agent service by replacing GLPI server url with a wrong url or disabling the service. Additionally, in the case the Deploy task is installed, a local malicious user can trigger privilege escalation configuring a malicious server providing its own deploy task payload. GLPI-Agent 1.7.2 contains a patch for this issue. As a workaround, edit GLPI-Agent related key under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` and add `SystemComponent` DWORD value setting it to `1` to hide GLPI-Agent from installed applications. | 7.3 | More Details |
| CVE-2024-4024 | An issue has been discovered in GitLab CE/EE affecting all versions starting from 7.8 before 16.9.6, all versions starting from 16.10 before 16.10.4, all versions starting from 16.11 before 16.11.1. Under certain conditions, an attacker with their Bitbucket account credentials may be able to take over a GitLab account linked to another user's Bitbucket account, if Bitbucket is used as an OAuth 2.0 provider on GitLab. | 7.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4298 | The email search interface of HGiga iSherlock (including MailSherlock, SpamSherock, AuditSherlock) fails to filter special characters in certain function parameters, allowing remote attackers with administrative privileges to exploit this vulnerability for Command Injection attacks, enabling execution of arbitrary system commands. | 7.2 | More Details |
| CVE-2024-28269 | ReCrystallize Server 5.10.0.0 allows administrators to upload files to the server. The file upload is not restricted, leading to the ability to upload of malicious files. This could result in a Remote Code Execution. | 7.2 | More Details |
| CVE-2024-4299 | The system configuration interface of HGiga iSherlock (including MailSherlock, SpamSherock, AuditSherlock) fails to filter special characters in certain function parameters, allowing remote attackers with administrative privileges to exploit this vulnerability for Command Injection attacks, enabling execution of arbitrary system commands. | 7.2 | More Details |
| CVE-2024-2617 | A vulnerability exists in the RTU500 that allows for authenticated and authorized users to bypass secure update. If a malicious actor successfully exploits this vulnerability, they could use it to update the RTU500 with unsigned firmware. | 7.2 | More Details |
| CVE-2024-3154 | A flaw was found in cri-o, where an arbitrary systemd property can be injected via a Pod annotation. Any user who can create a pod with an arbitrary annotation may perform an arbitrary action on the host system. | 7.2 | More Details |
| CVE-2024-1789 | The WP SMTP plugin for WordPress is vulnerable to SQL Injection via the 'search' parameter in versions 1.2 to 1.2.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | 7.2 | More Details |
| CVE-2024-33443 | An issue in onethink v.1.1 allows a remote attacker to execute arbitrary code via a crafted script to the AddonsController.class.php component. | 7.1 | More Details |
| CVE-2024-27791 | The issue was addressed with improved checks. This issue is fixed in iOS 17.3 and iPadOS 17.3, tvOS 17.3, macOS Ventura 13.6.4, iOS 16.7.5 and iPadOS 16.7.5, macOS Monterey 12.7.3, macOS Sonoma 14.3. An app may be able to corrupt coprocessor memory. | 7.1 | More Details |
| CVE-2023-52723 | In KDE libksieve before 23.03.80, kmanagesieve/session.cpp places a cleartext password in server logs because a username variable is accidentally given a password value. | 7.1 | More Details |
| CVE-2024-32958 | Cross-Site Request Forgery (CSRF) vulnerability in Giorgos Sarigiannidis Slash Admin allows Cross-Site Scripting (XSS).This issue affects Slash Admin: from n/a through 3.8.1. | 7.1 | More Details |
| CVE-2024-33645 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eftakhairul Islam & Sirajus Salayhin Easy Set Favicon allows Reflected XSS.This issue affects Easy Set Favicon: from n/a through 1.1. | 7.1 | More Details |
| CVE-2024-33646 | Cross-Site Request Forgery (CSRF) vulnerability in Toast Plugins Sticky Anything allows Cross-Site Scripting (XSS).This issue affects Sticky Anything: from n/a through 2.1.5. | 7.1 | More Details |
| CVE-2024-3371 | MongoDB Compass may accept and use insufficiently validated input from an untrusted external source. This may cause unintended application behavior, including data disclosure and enabling attackers to impersonate users. This issue affects MongoDB Compass versions 1.35.0 to 1.42.0. | 7.1 | More Details |
| CVE-2024-32785 | Cross-Site Request Forgery (CSRF) vulnerability in Webangon The Pack Elementor addons allows Cross-Site Scripting (XSS).This issue affects The Pack Elementor addons: from n/a through 2.0.8.3. | 7.1 | More Details |
| CVE-2024-33633 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Piotnet Piotnet Addons For Elementor Pro allows Reflected XSS.This issue affects Piotnet Addons For Elementor Pro: from n/a through 7.1.17. | 7.1 | More Details |
| CVE-2024-33258 | Jerryscript commit ff9ff8f was discovered to contain a segmentation violation via the component vm_loop at jerry-core/vm/vm.c. | 7.1 | More Details |
| CVE-2024-32492 | An issue was discovered in Znuny 7.0.1 through 7.0.16 where the ticket detail view in the customer front allows the execution of external JavaScript. | 7.1 | More Details |
| CVE-2024-4077 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AndonDesign UDesign allows Reflected XSS.This issue affects UDesign: from n/a through 4.7.3. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32789 | Cross-Site Request Forgery (CSRF) vulnerability in Seers allows Cross-Site Scripting (XSS).This issue affects Seers: from n/a through 8.1.0. | 7.1 | More Details |
| CVE-2024-32702 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Repute info systems ARForms allows Reflected XSS.This issue affects ARForms: from n/a through 6.4. | 7.1 | More Details |
| CVE-2024-33554 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore Core allows Reflected XSS.This issue affects XStore Core: from n/a through 5.3.5. | 7.1 | More Details |
| CVE-2024-33681 | Cross-Site Request Forgery (CSRF) vulnerability in Sandor Kovacs Regenerate post permalink allows Cross-Site Scripting (XSS).This issue affects Regenerate post permalink: from n/a through 1.0.3. | 7.1 | More Details |
| CVE-2024-32970 | Phlex is a framework for building object-oriented views in Ruby. In affected versions there is a potential cross-site scripting (XSS) vulnerability that can be exploited via maliciously crafted user data. Since the last two vulnerabilities https://github.com/phlex-ruby/phlex/security/advisories/GHSA-242p-4v39-2v8g and https://github.com/phlex-ruby/phlex/security/advisories/GHSA-g7xq-xv8c-h98c, we have invested in extensive browser tests. It was these new tests that helped us uncover these issues. As of now the project exercises every possible attack vector the developers can think of — including enumerating every ASCII character, and we run these tests in Chrome, Firefox and Safari. Additionally, we test against a list of 6613 known XSS payloads (see: payloadbox/xss-payload-list). The reason these issues were not detected before is the escapes were working as designed. However, their design didn't take into account just how recklessly permissive browsers are when it comes to executing unsafe JavaScript via HTML attributes. If you render an `<a>` tag with an `href` attribute set to a user-provided link, that link could potentially execute JavaScript when clicked by another user. If you splat user-provided attributes when rendering any HTML or SVG tag, malicious event attributes could be included in the output, executing JavaScript when the events are triggered by another user. Patches are available on RubyGems for all minor versions released in the last year. Users are advised to upgrade. Users unable to upgrade should configure a Content Security Policy that does not allow `unsafe-inline` which would effectively prevent this vulnerability from being exploited. Users who upgrade are also advised to configure a Content Security Policy header that does not allow `unsafe-inline`. | 7.1 | More Details |
| CVE-2024-33571 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Infomaniak Staff VOD Infomaniak allows Reflected XSS.This issue affects VOD Infomaniak: from n/a through 1.5.6. | 7.1 | More Details |
| CVE-2024-33562 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore allows Reflected XSS.This issue affects XStore: from n/a through 9.3.5. | 7.1 | More Details |
| CVE-2020-27478 | Cross Site Scripting vulnerability found in Simplcommerce v.40734964b0811f3cbaf64b6dac261683d256f961 thru 3103357200c70b4767986544e01b19dbf11505a7 allows a remote attacker to execute arbitrary code via a crafted script to the search bar feature. | 7.1 | More Details |
| CVE-2024-31609 | Cross Site Scripting (XSS) vulnerability in BOSSCMS v3.10 allows attackers to run arbitrary code via the header code and footer code fields in code configuration. | 7.1 | More Details |
| CVE-2024-33465 | Cross Site Scripting vulnerability in MajorDoMo before v.0662e5e allows an attacker to escalate privileges via the the thumb/thumb.php component. | 7.1 | More Details |
| CVE-2024-33548 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA-Team WZone allows Reflected XSS.This issue affects WZone: from n/a through 14.0.10. | 7.1 | More Details |
| CVE-2024-32950 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DeBAAT WP Media Category Management allows Reflected XSS.This issue affects WP Media Category Management: from n/a through 2.2. | 7.1 | More Details |
| CVE-2024-32952 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BloomPixel Max Addons Pro for Bricks allows Reflected XSS.This issue affects Max Addons Pro for Bricks: from n/a through 1.6.1. | 7.1 | More Details |
| CVE-2024-32878 | Llama.cpp is LLM inference in C/C++. There is a use of uninitialized heap variable vulnerability in gguf_init_from_file, the code will free this uninitialized variable later. In a simple POC, it will directly cause a crash. If the file is carefully constructed, it may be possible to control this uninitialized value and cause arbitrary address free problems. This may further lead to be exploited. Causes llama.cpp to crash (DoS) and may even lead to arbitrary code execution (RCE). This vulnerability has been patched in commit b2740. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-33899 | RARLAB WinRAR before 7.00, on Linux and UNIX platforms, allows attackers to spoof the screen output, or cause a denial of service, via ANSI escape sequences. | 7.1 | More Details |
| CVE-2024-33904 | In plugins/HookSystem.cpp in Hyprland through 0.39.1 (before 28c8561), through a race condition, a local attacker can cause execution of arbitrary assembly code by writing to a predictable temporary file. | 7.0 | More Details |
| CVE-2024-28326 | Incorrect Access Control in ASUS RT-N12+ B1 and RT-N12 D1 routers allows local attackers to obtain root terminal access via the the UART interface. | 6.8 | More Details |
| CVE-2024-30939 | An issue discovered in Yealink VP59 Teams Editions with firmware version 91.15.0.118 allows a physically proximate attacker to gain control of an account via a flaw in the factory reset procedure. | 6.8 | More Details |
| CVE-2024-25624 | Iris is a web collaborative platform aiming to help incident responders sharing technical details during investigations. Due to an improper setup of Jinja2 environment, reports generation in `iris-web` is prone to a Server Side Template Injection (SSTI). Successful exploitation of the vulnerability can lead to an arbitrary Remote Code Execution. An authenticated administrator has to upload a crafted report template containing the payload. Upon generation of a report based on the weaponized report, any user can trigger the vulnerability. The vulnerability is patched in IRIS v2.4.6. No workaround is available. It is recommended to update as soon as possible. Until patching, review the report templates and keep the administrative privileges that include the upload of report templates limited to dedicated users. | 6.8 | More Details |
| CVE-2024-33272 | SQL injection vulnerability in KnowBand for PrestaShop autosuggest before 2.0.0 allows an attacker to run arbitrary SQL commands via the AutosuggestSearchModuleFrontController::initContent(), and AutosuggestSearchModuleFrontController::getKbProducts() components. | 6.8 | More Details |
| CVE-2024-2907 | The AGCA WordPress plugin before 7.2.2 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). | 6.8 | More Details |
| CVE-2024-2859 | By default, SANnav OVA is shipped with root user login enabled. While protected by a password, access to root could expose SANnav to a remote attacker should they gain access to the root account. | 6.8 | More Details |
| CVE-2023-50914 | A Privilege Escalation issue in the inter-process communication procedure from GOG Galaxy (Beta) 2.0.67.2 through v2.0.71.2 allows authentictaed users to change the DACL of arbitrary system directories to include Everyone full control permissions by modifying the FixDirectoryPrivileges instruction parameters sent from GalaxyClient.exe to GalaxyClientService.exe. | 6.7 | More Details |
| CVE-2024-33522 | In vulnerable versions of Calico (v3.27.2 and below), Calico Enterprise (v3.19.0-1, v3.18.1, v3.17.3 and below), and Calico Cloud (v19.2.0 and below), an attacker who has local access to the Kubernetes node, can escalate their privileges by exploiting a vulnerability in the Calico CNI install binary. The issue arises from an incorrect SUID (Set User ID) bit configuration in the binary, combined with the ability to control the input binary, allowing an attacker to execute an arbitrary binary with elevated privileges. | 6.7 | More Details |
| CVE-2024-3196 | A vulnerability was found in MailCleaner up to 2023.03.14. It has been declared as critical. This vulnerability affects the function getStats/Services_silentDump/Services_stopStartMTA/Config_saveDateTime/Config_hostid/Logs_StartGetStat/dumpConfiguration of the component SOAP Service. The manipulation leads to os command injection. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-262312. | 6.7 | More Details |
| CVE-2024-23772 | An issue was discovered in Quest KACE Agent for Windows 12.0.38 and 13.1.23.0. An Arbitrary file create vulnerability exists in the KSchedulerSvc.exe, KUserAlert.exe, and Runkbot.exe components. This allows local attackers to create any file of their choice with NT Authority\SYSTEM privileges. | 6.6 | More Details |
| CVE-2023-5675 | A flaw was found in Quarkus. When a Quarkus RestEasy Classic or Reactive JAX-RS endpoint has its methods declared in the abstract Java class or customized by Quarkus extensions using the annotation processor, the authorization of these methods will not be enforced if it is enabled by either 'quarkus.security.jaxrs.deny-unannotated-endpoints' or 'quarkus.security.jaxrs.default-roles-allowed' properties. | 6.5 | More Details |
| CVE-2024-33667 | An issue was discovered in Zammad before 6.3.0. An authenticated agent could perform a remote Denial of Service attack by calling an endpoint that accepts a generic method name, which was not properly sanitized against an allowlist. | 6.5 | More Details |
| CVE-2024-25569 | An out-of-bounds read vulnerability exists in the RAWCodec::DecodeBytes functionality of Mathieu Malaterre Grassroot DICOM 3.0.23. A specially crafted DICOM file can lead to an out-of-bounds read. An attacker can provide a malicious file to trigger this vulnerability. | 6.5 | More Details |
| CVE-2024-33558 | Missing Authorization vulnerability in 8theme XStore Core.This issue affects XStore Core: from n/a through 5.3.5. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-33684 | Missing Authorization vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This issue affects Save as PDF plugin by Pdfcrowd: from n/a through 3.2.0. | 6.5 | More Details |
| CVE-2024-1371 | The LeadConnector plugin for WordPress is vulnerable to unauthorized modification & loss of data due to a missing capability check on the lc_public_api_proxy() function in all versions up to, and including, 1.7. This makes it possible for unauthenticated attackers to delete arbitrary posts. | 6.5 | More Details |
| CVE-2024-32961 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative Themes HQ Blocksy allows Stored XSS.This issue affects Blocksy: from n/a through 2.0.33. | 6.5 | More Details |
| CVE-2024-32791 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.10.25. | 6.5 | More Details |
| CVE-2024-33589 | Missing Authorization vulnerability in WPOmnia KB Support.This issue affects KB Support: from n/a through 1.6.0. | 6.5 | More Details |
| CVE-2023-6787 | A flaw was found in Keycloak that occurs from an error in the re-authentication mechanism within org.keycloak.authentication. This flaw allows hijacking an active Keycloak session by triggering a new authentication process with the query parameter "prompt=login," prompting the user to re-enter their credentials. If the user cancels this re-authentication by selecting "Restart login," an account takeover may occur, as the new session, with a different SUB, will possess the same SID as the previous session. | 6.5 | More Details |
| CVE-2024-1102 | A vulnerability was found in jberet-core logging. An exception in 'dbProperties' might display user credentials such as the username and password for the database-connection. | 6.5 | More Details |
| CVE-2024-32868 | ZITADEL provides users the possibility to use Time-based One-Time-Password (TOTP) and One-Time-Password (OTP) through SMS and Email. While ZITADEL already gives administrators the option to define a `Lockout Policy` with a maximum amount of failed password check attempts, there was no such mechanism for (T)OTP checks. This issue has been patched in version 2.50.0. | 6.5 | More Details |
| CVE-2023-50915 | An issue exists in GalaxyClientService.exe in GOG Galaxy (Beta) 2.0.67.2 through 2.0.71.2 that could allow authenticated users to overwrite and corrupt critical system files via a combination of an NTFS Junction and an RPC Object Manager symbolic link and could result in a denial of service. | 6.5 | More Details |
| CVE-2024-32711 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in myCred allows Stored XSS.This issue affects myCred: from n/a through 2.6.3. | 6.5 | More Details |
| CVE-2024-33537 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Theme Horse WP Portfolio allows Stored XSS.This issue affects WP Portfolio: from n/a through 2.4. | 6.5 | More Details |
| CVE-2022-45852 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in FormAssembly / Drew Buschhorn WP-FormAssembly allows Path Traversal.This issue affects WP-FormAssembly: from n/a through 2.0.5. | 6.5 | More Details |
| CVE-2024-32721 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jegtheme Jeg Elementor Kit allows Stored XSS.This issue affects Jeg Elementor Kit: from n/a through 2.6.3. | 6.5 | More Details |
| CVE-2024-32956 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rometheme RomethemeKit For Elementor allows Stored XSS.This issue affects RomethemeKit For Elementor: from n/a through 1.4.1. | 6.5 | More Details |
| CVE-2024-33539 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPZOOM WPZOOM Addons for Elementor (Templates, Widgets) allows Stored XSS.This issue affects WPZOOM Addons for Elementor (Templates, Widgets): from n/a through 1.1.35. | 6.5 | More Details |
| CVE-2024-33540 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGrill ColorNews allows Stored XSS.This issue affects ColorNews: from n/a through 1.2.6. | 6.5 | More Details |
| CVE-2023-52726 | Open Networking Foundation SD-RAN ONOS onos-ric-sdk-go 0.8.12 allows infinite repetition of the processing of an error (in the Subscribe function implementation for the subscribed indication stream). | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-52725 | Open Networking Foundation SD-RAN ONOS onos-kpimon 0.4.7 allows blocking of the errCh channel within the Start function of the monitoring package. | 6.5 | More Details |
| CVE-2024-32675 | Missing Authorization vulnerability in Xfinity Soft Order Limit for WooCommerce.This issue affects Order Limit for WooCommerce: from n/a through 2.0.0. | 6.5 | More Details |
| CVE-2024-0151 | Insufficient argument checking in Secure state Entry functions in software using Cortex-M Security Extensions (CMSE), that has been compiled using toolchains that implement 'Arm v8-M Security Extensions Requirements on Development Tools' prior to version 1.4, allows an attacker to pass values to Secure state that are out of range for types smaller than 32-bits. Out of range values might lead to incorrect operations in secure state. | 6.5 | More Details |
| CVE-2024-21905 | An integer overflow or wraparound vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later | 6.5 | More Details |
| CVE-2024-33631 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Piotnet Piotnet Addons For Elementor Pro allows Stored XSS.This issue affects Piotnet Addons For Elementor Pro: from n/a through 7.1.17. | 6.5 | More Details |
| CVE-2024-2756 | Due to an incomplete fix to CVE-2022-31629 https://github.com/advisories/GHSA-c43m-486j-j32p , network and same-site attackers can set a standard insecure cookie in the victim's browser which is treated as a __Host- or __Secure- cookie by PHP applications. | 6.5 | More Details |
| CVE-2024-33345 | D-Link DIR-823G A1V1.0.2B05 was found to contain a Null-pointer dereference in the main function of upload_firmware.cgi, which allows remote attackers to cause a Denial of Service (DoS) via a crafted input. | 6.5 | More Details |
| CVE-2024-3096 | In PHP  version 8.1.* before 8.1.28, 8.2.* before 8.2.18, 8.3.* before 8.3.5, if a password stored with password_hash() starts with a null byte (\x00), testing a blank string as the password via password_verify() will incorrectly return true. | 6.5 | More Details |
| CVE-2024-32051 | Insertion of sensitive information into log file issue exists in RoamWiFi R10 prior to 4.8.45. If this vulnerability is exploited, a network-adjacent unauthenticated attacker with access to the device may obtain sensitive information. | 6.5 | More Details |
| CVE-2024-33640 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LBell Pretty Google Calendar allows Stored XSS.This issue affects Pretty Google Calendar: from n/a through 1.7.2. | 6.5 | More Details |
| CVE-2024-28294 | Limbas up to v5.2.14 was discovered to contain a SQL injection vulnerability via the ftid parameter. | 6.5 | More Details |
| CVE-2023-50433 | marshall in dhcp_packet.c in simple-dhcp-server through ec976d2 allows remote attackers to cause a denial of service by sending a malicious DHCP packet. The crash is caused by a type confusion bug that results in a large memory allocation; when this memory allocation fails the DHCP server will crash. | 6.5 | More Details |
| CVE-2024-33630 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Piotnet Piotnet Addons For Elementor allows Stored XSS.This issue affects Piotnet Addons For Elementor: from n/a through 2.4.26. | 6.5 | More Details |
| CVE-2024-32677 | Missing Authorization vulnerability in LoginPress LoginPress Pro.This issue affects LoginPress Pro: from n/a before 3.0.0. | 6.5 | More Details |
| CVE-2024-34020 | A stack-based buffer overflow was found in the putSDN() function of mail.c in hcode through 2.1. | 6.5 | More Details |
| CVE-2024-33648 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wzy Media Recencio Book Reviews allows Stored XSS.This issue affects Recencio Book Reviews: from n/a through 1.66.0. | 6.5 | More Details |
| CVE-2024-32951 | Missing Authorization vulnerability in BloomPixel Max Addons Pro for Bricks.This issue affects Max Addons Pro for Bricks: from n/a through 1.6.1. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4292 | A vulnerability classified as critical has been found in Contemporary Controls BASrouter BACnet BASRT-B 2.7.2. Affected is an unknown function of the component Device-Communication-Control Service. The manipulation with the input 55ff0500370015f30104025506110afb7519035d0841e4bece257b6acfc71f leads to denial of service. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-262224. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 6.5 | More Details |
| CVE-2024-23271 | A logic issue was addressed with improved checks. This issue is fixed in iOS 17.3 and iPadOS 17.3, Safari 17.3, tvOS 17.3, macOS Sonoma 14.3, watchOS 10.3. A malicious website may cause unexpected cross-origin behavior. | 6.5 | More Details |
| CVE-2024-33649 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WpOpal Opal Widgets For Elementor allows Stored XSS.This issue affects Opal Widgets For Elementor: from n/a through 1.6.9. | 6.5 | More Details |
| CVE-2024-33663 | python-jose through 3.3.0 has algorithm confusion with OpenSSH ECDSA keys and other key formats. This is similar to CVE-2022-29217. | 6.5 | More Details |
| CVE-2023-50364 | A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later | 6.4 | More Details |
| CVE-2024-32803 | Server-Side Request Forgery (SSRF) vulnerability in 2day.Sk, Webikon SuperFaktura WooCommerce.This issue affects SuperFaktura WooCommerce: from n/a through 1.40.3. | 6.4 | More Details |
| CVE-2024-22546 | TRENDnet TEW-815DAP 1.0.2.0 is vulnerable to Command Injection via the do_setNTP function. An authenticated attacker with administrator privileges can leverage this vulnerability over the network via a malicious POST request. | 6.4 | More Details |
| CVE-2024-4035 | The Photo Gallery – GT3 Image Gallery & Gutenberg Block Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image alt text in all versions up to, and including, 2.7.7.21 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-2024-2838 | The WPC Composite Products for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wooco_components[0][name]' parameter in all versions up to, and including, 7.2.7 due to insufficient input sanitization and output escaping and missing authorization on the ajax_save_components function. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2024-3309 | The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown Widget's attributes in all versions up to, and including, 1.7.0 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-2024-0216 | The Google Doc Embedder plugin for WordPress is vulnerable to Server Side Request Forgery via the 'gview' shortcode in versions up to, and including, 2.6.4. This can allow authenticated attackers with contributor-level permissions or 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. | 6.4 | More Details |
| CVE-2024-3890 | The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Calendly widget in all versions up to, and including, 3.10.5 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-2024-3929 | The Content Views – Post Grid & Filter, Recent Posts, Category Posts, & More (Gutenberg Blocks and Shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Widget Post Overlay block in all versions up to, and including, 3.7.0 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-2024-3988 | The Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Sina Fancy Text Widget in all versions up to, and including, 3.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32884 | gitoxide is a pure Rust implementation of Git. `gix-transport` does not check the username part of a URL for text that the external `ssh` program would interpret as an option. A specially crafted clone URL can smuggle options to SSH. The possibilities are syntactically limited, but if a malicious clone URL is used by an application whose current working directory contains a malicious file, arbitrary code execution occurs. This is related to the patched vulnerability GHSA-rrjw-j4m2-mf34, but appears less severe due to a greater attack complexity. This issue has been patched in versions 0.35.0, 0.42.0 and 0.62.0. | 6.4 | More Details |
| CVE-2023-1000 | A vulnerability was found in cyanomiko dcnnt-py up to 0.9.0. It has been classified as critical. Affected is the function main of the file dcnnt/plugins/notifications.py of the component Notification Handler. The manipulation leads to command injection. It is possible to launch the attack remotely. Upgrading to version 0.9.1 is able to address this issue. The patch is identified as b4021d784a97e25151a5353aa763a741e9a148f5. It is recommended to upgrade the affected component. VDB-262230 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2024-33832 | OneNav v0.9.35-20240318 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /index.php?c=api&method=get_link_info. | 6.3 | More Details |
| CVE-2024-4257 | A vulnerability was found in BlueNet Technology Clinical Browsing System 1.2.1. It has been classified as critical. This affects an unknown part of the file /xds/deleteStudy.php. The manipulation of the argument documentUniqueId 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-262149 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2024-4310 | Cross-site Scripting (XSS) vulnerability in HubBank affecting version 1.0.2. This vulnerability allows an attacker to send a specially crafted JavaScript payload to registration and profile forms and trigger the payload when any authenticated user loads the page, resulting in a session takeover. | 6.3 | More Details |
| CVE-2024-4294 | A vulnerability, which was classified as critical, has been found in PHPGurukul Doctor Appointment Management System 1.0. Affected by this issue is some unknown functionality of the file /doctor/view-appointment-detail.php. The manipulation of the argument editid leads to improper control of resource identifiers. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-262226 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2024-28961 | Dell OpenManage Enterprise, versions 4.0.0 and 4.0.1, contains a sensitive information disclosure vulnerability. A local low privileged malicious user could potentially exploit this vulnerability to obtain credentials leading to unauthorized access with elevated privileges. This could lead to further attacks, thus Dell recommends customers to upgrade at the earliest opportunity. | 6.3 | More Details |
| CVE-2024-34149 | In Bitcoin Core through 27.0 and Bitcoin Knots before 25.1.knots20231115, tapscript lacks a policy size limit check, a different issue than CVE-2023-50428. NOTE: some parties oppose this new limit check (for example, because they agree with the objective but disagree with the technical mechanism, or because they have a different objective). | 6.3 | More Details |
| CVE-2024-4093 | A vulnerability, which was classified as critical, was found in SourceCodester Simple Subscription Website 1.0. Affected is an unknown function of the file view_application.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-261822 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2024-31610 | File Upload vulnerability in the function for employees to upload avatars in Code-Projects Simple School Management System v1.0 allows attackers to run arbitrary code via upload of crafted file. | 6.3 | More Details |
| CVE-2024-3188 | The WP Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 7.1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 6.3 | More Details |
| CVE-2024-2603 | The Salon booking system WordPress plugin through 9.6.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin (or editor depending on Salon booking system WordPress plugin through 9.6.5 configuration) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | 6.3 | More Details |
| CVE-2023-47252 | An issue was discovered in PnpSmm in Insyde InsydeH2O with kernel 5.0 through 5.6. There is a possible out-of-bounds access in the SMM communication buffer, leading to tampering. The PNP-related SMI sub-functions do not verify data size before getting it from the communication buffer, which could lead to possible circumstances where the data immediately following the command buffer could be destroyed with a fixed value. This is fixed in kernel 5.2 v05.28.45, kernel 5.3 v05.37.45, kernel 5.4 v05.45.45, kernel 5.5 v05.53.45, and kernel 5.6 v05.60.45. | 6.3 | More Details |
| CVE-2024-0905 | The Fancy Product Designer WordPress plugin before 6.1.8 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 unauthenticated and admin-level users | 6.3 | More Details |
| CVE-2024-33255 | Jerryscript commit cefd391 was discovered to contain an Assertion Failure via ECMA_STRING_IS_REF_EQUALS_TO_ONE (string_p) in ecma_free_string_list. | 6.2 | More Details |
| CVE-2024-2905 | A security vulnerability has been discovered within rpm-ostree, pertaining to the /etc/shadow file in default builds having the world-readable bit enabled. This issue arises from the default permissions being set at a higher level than recommended, potentially exposing sensitive authentication data to unauthorized access. | 6.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-28963 | Telemetry Dashboard v1.0.0.7 for Dell ThinOS 2402 contains a sensitive information disclosure vulnerability. An unauthenticated user with local access to the device could exploit this vulnerability to read sensitive proxy settings information. | 6.2 | More Details |
| CVE-2022-48635 | In the Linux kernel, the following vulnerability has been resolved: fsdax: Fix infinite loop in dax_iomap_rw() I got an infinite loop and a WARNING report when executing a tail command in virtiofs. WARNING: CPU: 10 PID: 964 at fs/iomap/iter.c:34 iomap_iter+0x3a2/0x3d0 Modules linked in: CPU: 10 PID: 964 Comm: tail Not tainted 5.19.0-rc7 Call Trace: <TASK> dax_iomap_rw+0xea/0x620 ? __this_cpu_preempt_check+0x13/0x20 fuse_dax_read_iter+0x47/0x80 fuse_file_read_iter+0xae/0xd0 new_sync_read+0xfe/0x180 ? 0xffffffff81000000 vfs_read+0x14d/0x1a0 ksys_read+0x6d/0xf0 __x64_sys_read+0x1a/0x20 do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd The tail command will call read() with a count of 0. In this case, iomap_iter() will report this WARNING, and always return 1 which casuing the infinite loop in dax_iomap_rw(). Fixing by checking count whether is 0 in dax_iomap_rw(). | 6.2 | More Details |
| CVE-2022-48646 | In the Linux kernel, the following vulnerability has been resolved: sfc/siena: fix null pointer dereference in efx_hard_start_xmit Like in previous patch for sfc, prevent potential (but unlikely) NULL pointer dereference. | 6.2 | More Details |
| CVE-2023-51254 | Cross Site Scripting vulnerability in Jfinalcms v.5.0.0 allows a remote attacker to execute arbitrary code via a crafted script to the friendship link component. | 6.1 | More Details |
| CVE-2024-28325 | Asus RT-N12+ B1 router stores credentials in cleartext, which could allow local attackers to obtain unauthorized access and modify router settings. | 6.1 | More Details |
| CVE-2024-31741 | Cross Site Scripting vulnerability in MiniCMS v.1.11 allows a remote attacker to run arbitrary code via crafted string in the URL after login. | 6.1 | More Details |
| CVE-2024-33103 | An arbitrary file upload vulnerability in the Media Manager component of DokuWiki 2024-02-06a allows attackers to execute arbitrary code by uploading a crafted SVG file. NOTE: as noted in the 4267 issue reference, there is a position that exploitability can only occur with a misconfiguration of the product. | 6.1 | More Details |
| CVE-2023-7253 | The Import WP WordPress plugin before 2.13.1 does not prevent users with the administrator role from pinging conducting SSRF attacks, which may be a problem in multisite configurations. | 6.1 | More Details |
| CVE-2024-33101 | A stored cross-site scripting (XSS) vulnerability in the component /action/anti.php of ThinkSAAS v3.7.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the word parameter. | 6.1 | More Details |
| CVE-2024-4302 | Super 8 Live Chat online customer service platform fails to properly filter user input, allowing unauthenticated remote attackers to insert JavaScript code into the chat box. When the message recipient views the message, they become susceptible to Cross-site Scripting (XSS) attacks. | 6.1 | More Details |
| CVE-2024-33669 | An issue was discovered in Passbolt Browser Extension before 4.6.2. It can send multiple requests to HaveIBeenPwned while a password is being typed, which results in an information leak. This allows an attacker capable of observing Passbolt's HTTPS queries to the Pwned Password API to more easily brute force passwords that are manually typed by the user. | 6.1 | More Details |
| CVE-2024-33665 | angular-translate through 2.19.1 allows XSS via a crafted key that is used by the translate directive. NOTE: the vendor indicates that there is no documentation indicating that a key is supposed to be safe against XSS attacks. | 6.1 | More Details |
| CVE-2024-23995 | Cross Site Scripting (XSS) in Beekeeper Studio 4.1.13 and earlier allows remote attackers to execute arbitrary code in the column name of a database table in tabulator-popup-container. | 6.1 | More Details |
| CVE-2024-31828 | Cross Site Scripting vulnerability in Lavalite CMS v.10.1.0 allows attackers to execute arbitrary code and obtain sensitive information via a crafted payload to the URL. | 6.1 | More Details |
| CVE-2024-33371 | Cross Site Scripting vulnerability in DedeCMS v.5.7.113 allows a remote attacker to execute arbitrary code via the typeid parameter in the makehtml_list_action.php component. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-20359 | A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. | 6.0 | More Details |
| CVE-2024-32404 | Server-Side Template Injection (SSTI) vulnerability in inducer relate before v.2024.1, allows remote attackers to execute arbitrary code via a crafted payload to the Markup Sandbox feature. | 6.0 | More Details |
| CVE-2024-20358 | A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root. | 6.0 | More Details |
| CVE-2022-48682 | In deletefiles in FDUPES before 2.2.0, a TOCTOU race condition allows arbitrary file deletion via a symlink. | 6.0 | More Details |
| CVE-2023-6717 | A flaw was found in the SAML client registration in Keycloak that could allow an administrator to register malicious JavaScript URIs as Assertion Consumer Service POST Binding URLs (ACS), posing a Cross-Site Scripting (XSS) risk. This issue may allow a malicious admin in one realm or a client with registration access to target users in different realms or applications, executing arbitrary JavaScript in their contexts upon form submission. This can enable unauthorized access and harmful actions, compromising the confidentiality, integrity, and availability of the complete KC instance. | 6.0 | More Details |
| CVE-2020-5200 | Minerbabe through V4.16 ships with SSH host keys baked into the installation image, which allows man-in-the-middle attacks and makes identification of all public IPv4 nodes trivial with Shodan.io. | 5.9 | More Details |
| CVE-2024-32815 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Peters All-in-one Like Widget allows Stored XSS.This issue affects All-in-one Like Widget: from n/a through 2.2.7. | 5.9 | More Details |
| CVE-2024-32801 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin Widget Post Slider allows Stored XSS.This issue affects Widget Post Slider: from n/a through 1.3.5. | 5.9 | More Details |
| CVE-2024-33598 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Twinpictures Annual Archive allows Stored XSS.This issue affects Annual Archive: from n/a through 1.6.0. | 5.9 | More Details |
| CVE-2024-33642 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EkoJR Advanced Post List allows Stored XSS.This issue affects Advanced Post List: from n/a through 0.5.6.1. | 5.9 | More Details |
| CVE-2024-32833 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Halsey List Custom Taxonomy Widget allows Stored XSS.This issue affects List Custom Taxonomy Widget: from n/a through 4.1. | 5.9 | More Details |
| CVE-2024-32834 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebToffee WooCommerce Shipping Label allows Stored XSS.This issue affects WooCommerce Shipping Label: from n/a through 2.3.8. | 5.9 | More Details |
| CVE-2024-32722 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Coupon & Discount Code Reveal Button allows Stored XSS.This issue affects Coupon & Discount Code Reveal Button: from n/a through 1.2.5. | 5.9 | More Details |
| CVE-2024-33639 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AccessAlly PopupAlly allows Stored XSS.This issue affects PopupAlly: from n/a through 2.1.1. | 5.9 | More Details |
| CVE-2024-33903 | In CARLA through 0.9.15.2, the collision sensor mishandles some situations involving pedestrians or bicycles, in part because the collision sensor function is not exposed to the Blueprint library. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32723 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Code Tides Advanced Floating Content allows Stored XSS.This issue affects Advanced Floating Content: from n/a through 1.2.5. | 5.9 | More Details |
| CVE-2024-32780 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in E4J s.R.L. VikRentCar.This issue affects VikRentCar: from n/a through 1.3.2. | 5.9 | More Details |
| CVE-2024-32707 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Image Slider Widget allows Stored XSS.This issue affects Image Slider Widget: from n/a through 1.1.125. | 5.9 | More Details |
| CVE-2024-25026 | IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.4 are vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 281516. | 5.9 | More Details |
| CVE-2024-33643 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kailey Lampert Advanced Most Recent Posts Mod allows Stored XSS.This issue affects Advanced Most Recent Posts Mod: from n/a through 1.6.5.2. | 5.9 | More Details |
| CVE-2024-33694 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Meks Meks ThemeForest Smart Widget allows Stored XSS.This issue affects Meks ThemeForest Smart Widget: from n/a through 1.5. | 5.9 | More Details |
| CVE-2023-26603 | JumpCloud Agent before 1.178.0 Creates a Temporary File in a Directory with Insecure Permissions. This allows privilege escalation to SYSTEM via a repair action in the installer. | 5.9 | More Details |
| CVE-2024-4234 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sayful Islam Filterable Portfolio allows Stored XSS.This issue affects Filterable Portfolio: from n/a through 1.6.4. | 5.9 | More Details |
| CVE-2024-33697 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rimes Gold CF7 File Download – File Download for CF7 allows Stored XSS.This issue affects CF7 File Download – File Download for CF7: from n/a through 2.0. | 5.9 | More Details |
| CVE-2024-33696 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Broadstreet XPRESS WordPress Ad Widget allows Stored XSS.This issue affects WordPress Ad Widget: from n/a through 2.20.0. | 5.9 | More Details |
| CVE-2024-33695 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNcode Fan Page Widget by ThemeNcode allows Stored XSS.This issue affects Fan Page Widget by ThemeNcode: from n/a through 2.0. | 5.9 | More Details |
| CVE-2024-33693 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Meks Meks Smart Social Widget allows Stored XSS.This issue affects Meks Smart Social Widget: from n/a through 1.6.4. | 5.9 | More Details |
| CVE-2024-33692 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Satrya Smart Recent Posts Widget allows Stored XSS.This issue affects Smart Recent Posts Widget: from n/a through 1.0.3. | 5.9 | More Details |
| CVE-2023-6237 | Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary: Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26924 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo: do not free live element Pablo reports a crash with large batches of elements with a back-to-back add/remove pattern. Quoting Pablo: add_elem("00000000") timeout 100 ms ... add_elem("0000000X") timeout 100 ms del_elem("0000000X") <---------- delete one that was just added ... add_elem("00005000") timeout 100 ms 1) nft_pipapo_remove() removes element 0000000X Then, KASAN shows a splat. Looking at the remove function there is a chance that we will drop a rule that maps to a non-deactivated element. Removal happens in two steps, first we do a lookup for key k and return the to-be-removed element and mark it as inactive in the next generation. Then, in a second step, the element gets removed from the set/map. The _remove function does not work correctly if we have more than one element that share the same key. This can happen if we insert an element into a set when the set already holds an element with same key, but the element mapping to the existing key has timed out or is not active in the next generation. In such case its possible that removal will unmap the wrong element. If this happens, we will leak the non-deactivated element, it becomes unreachable. The element that got deactivated (and will be freed later) will remain reachable in the set data structure, this can result in a crash when such an element is retrieved during lookup (stale pointer). Add a check that the fully matching key does in fact map to the element that we have marked as inactive in the deactivation step. If not, we need to continue searching. Add a bug/warn trap at the end of the function as well, the remove function must not ever be called with an invisible/unreachable/non-existent element. v2: avoid uneeded temporary variable (Stefano) | 5.9 | More Details |
| CVE-2024-28825 | Improper restriction of excessive authentication attempts on some authentication methods in Checkmk before 2.3.0b5 (beta), 2.2.0p26, 2.1.0p43, and in Checkmk 2.0.0 (EOL) facilitates password brute-forcing. | 5.9 | More Details |
| CVE-2024-2310 | The WP Google Review Slider WordPress plugin before 13.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | 5.9 | More Details |
| CVE-2024-2467 | A timing-based side-channel flaw exists in the perl-Crypt-OpenSSL-RSA package, which could be sufficient to recover plaintext across a network in a Bleichenbacher-style attack. To achieve successful decryption, an attacker would have to be able to send a large number of trial messages. The vulnerability affects the legacy PKCS#1v1.5 RSA encryption padding mode. | 5.9 | More Details |
| CVE-2024-1743 | The WooCommerce Customers Manager WordPress plugin before 29.8 does not sanitise and escape various parameters before outputting them back in pages and attributes, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin | 5.9 | More Details |
| CVE-2024-32467 | MeterSphere is an open source continuous testing platform. Prior to version 2.10.14-lts, members without space permissions can view member information from other workspaces beyond their authority. Version 2.10.14-lts fixes this issue. | 5.7 | More Details |
| CVE-2019-19754 | HiveOS through 0.6-102@191212 ships with SSH host keys baked into the installation image, which allows man-in-the-middle attacks and makes identification of all public IPv4 nodes trivial with Shodan.io. NOTE: as of 2019-09-26, the vendor indicated that they would consider fixing this. | 5.7 | More Details |
| CVE-2024-3059 | The ENL Newsletter WordPress plugin through 1.0.1 does not have CSRF checks in some places, which could allow attackers to make logged in admins delete arbitrary Campaigns via a CSRF attack | 5.7 | More Details |
| CVE-2024-32872 | Umbraco workflow provides workflows for the Umbraco content management system. Prior to versions 10.3.9, 12.2.6, and 13.0.6, an Umbraco Backoffice user can modify requests to a particular API endpoint to include SQL, which will be executed by the server. Umbraco Workflow versions 10.3.9, 12.2.6, 13.0.6, as well as Umbraco Plumber version 10.1.2, contain a patch for this issue. | 5.5 | More Details |
| CVE-2024-33259 | Jerryscript commit cefd391 was discovered to contain a segmentation violation via the component scanner_seek at jerry-core/parser/js/js-scanner-util.c. | 5.5 | More Details |
| CVE-2024-3048 | The Bannerlid WordPress plugin through 1.1.0 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as administrators | 5.5 | More Details |
| CVE-2022-48654 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_osf: fix possible bogus match in nf_osf_find() nf_osf_find() incorrectly returns true on mismatch, this leads to copying uninitialized memory area in nft_osf which can be used to leak stale kernel stack data to userspace. | 5.5 | More Details |
| CVE-2022-48656 | In the Linux kernel, the following vulnerability has been resolved: dmaengine: ti: k3-udma-private: Fix refcount leak bug in of_xudma_dev_get() We should call of_node_put() for the reference returned by of_parse_phandle() in fail path or when it is not used anymore. Here we only need to move the of_node_put() before the check. | 5.5 | More Details |
| CVE-2022-48660 | In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Set lineevent_state::irq after IRQ register successfully When running gpio test on nxp-ls1028 platform with below command gpiomon --num-events=3 --rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x70 gpio_ioctl+0x598/0x6a0 __arm64_sys_ioctl+0xb4/0x100 invoke_syscall+0x5c/0x130 ..... el0t_64_sync+0x1a0/0x1a4 The reason of this issue is that calling request_threaded_irq() function failed, and then lineevent_free() is invoked to release the resource. Since the lineevent_state::irq was already set, so the subsequent invocation of free_irq() would trigger the above warning call trace. To fix this issue, set the lineevent_state::irq after the IRQ register successfully. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48661 | In the Linux kernel, the following vulnerability has been resolved: gpio: mockup: Fix potential resource leakage when register a chip If creation of software node fails, the locally allocated string array is left unfreed. Free it on error path. | 5.5 | More Details |
| CVE-2023-52728 | Open Networking Foundation SD-RAN ONOS onos-lib-go 0.10.25 allows an index out-of-range condition in putBitString. | 5.5 | More Details |
| CVE-2023-31889 | An issue discovered in httpd in ASUS RT-AC51U with firmware version up to and including 3.0.0.4.380.8591 allows local attackers to cause a denial of service via crafted GET request. | 5.5 | More Details |
| CVE-2024-22405 | XADMaster is an objective-C library for archive and file unarchiving and extraction. When extracting a specially crafted zip archive XADMaster may not apply quarantine attribute correctly. Such behaviour may circumvent Gatekeeper checks on the system. Only macOS installations are affected. This issue was fixed in XADMaster 1.10.8. It is recommended to upgrade to the latest version. There are no known workarounds for this issue. | 5.5 | More Details |
| CVE-2022-48659 | In the Linux kernel, the following vulnerability has been resolved: mm/slub: fix to return errno if kmalloc() fails In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to out-of-memory, if it fails, return errno correctly rather than triggering panic via BUG_ON(); kernel BUG at mm/slub.c:5893! Internal error: Oops - BUG: 0 [#1] PREEMPT SMP Call trace: sysfs_slab_add+0x258/0x260 mm/slub.c:5973 __kmem_cache_create+0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 fs/namespace.c:3370 do_mount fs/namespace.c:3383 [inline] __do_sys_mount fs/namespace.c:3591 [inline] __se_sys_mount fs/namespace.c:3568 [inline] __arm64_sys_mount+0x2f8/0x408 fs/namespace.c:3568 | 5.5 | More Details |
| CVE-2024-2877 | Vault Enterprise, when configured with performance standby nodes and a configured audit device, will inadvertently log request headers on the standby node. These logs may have included sensitive HTTP request information in cleartext. This vulnerability, CVE-2024-2877, was fixed in Vault Enterprise 1.15.8. | 5.5 | More Details |
| CVE-2023-41291 | A path traversal vulnerability has been reported to affect QuFirewall. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following version: QuFirewall 2.4.1 ( 2024/02/01 ) and later | 5.5 | More Details |
| CVE-2022-48636 | In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix Oops in dasd_alias_get_start_dev due to missing pavgroup Fix Oops in dasd_alias_get_start_dev() function caused by the pavgroup pointer being NULL. The pavgroup pointer is checked on the entrance of the function but without the lcu->lock being held. Therefore there is a race window between dasd_alias_get_start_dev() and _lcu_update() which sets pavgroup to NULL with the lcu->lock held. Fix by checking the pavgroup pointer with lcu->lock held. | 5.5 | More Details |
| CVE-2024-32887 | Sidekiq is simple, efficient background processing for Ruby. Sidekiq is reflected XSS vulnerability. The value of substr parameter is reflected in the response without any encoding, allowing an attacker to inject Javascript code into the response of the application. An attacker could exploit it to target users of the Sidekiq Web UI. Moreover, if other applications are deployed on the same domain or website as Sidekiq, users of those applications could also be affected, leading to a broader scope of compromise. Potentially compromising their accounts, forcing the users to perform sensitive actions, stealing sensitive data, performing CORS attacks, defacement of the web application, etc. This issue has been patched in version 7.2.4. | 5.5 | More Details |
| CVE-2023-52722 | An issue was discovered in Artifex Ghostscript before 10.03.1. psi/zmisc1.c, when SAFER mode is used, allows eexec seeds other than the Type 1 standard. | 5.5 | More Details |
| CVE-2024-3746 | The entire parent directory - C:\ScadaPro and its sub-directories and files are configured by default to allow user, including unprivileged users, to write or overwrite files. | 5.5 | More Details |
| CVE-2024-33592 | Server-Side Request Forgery (SSRF) vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73. | 5.4 | More Details |
| CVE-2024-33102 | A stored cross-site scripting (XSS) vulnerability in the component /pubs/counter.php of ThinkSAAS v3.7.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the code parameter. | 5.4 | More Details |
| CVE-2024-2402 | The Better Comments WordPress plugin before 1.5.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-33634 | Server-Side Request Forgery (SSRF) vulnerability in Piotnet Piotnet Addons For Elementor Pro.This issue affects Piotnet Addons For Elementor Pro: from n/a through 7.1.17. | 5.4 | More Details |
| CVE-2024-3730 | The Simple Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'swpm_paypal_subscription_cancel_link' shortcode in all versions up to, and including, 4.4.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 5.4 | More Details |
| CVE-2024-3058 | The ENL Newsletter WordPress plugin through 1.0.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack | 5.4 | More Details |
| CVE-2024-2837 | The WP Chat App WordPress plugin before 3.6.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admins to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed | 5.4 | More Details |
| CVE-2023-20248 | A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. | 5.4 | More Details |
| CVE-2024-33641 | Deserialization of Untrusted Data vulnerability in Team Yoast Custom field finder.This issue affects Custom field finder: from n/a through 0.3. | 5.4 | More Details |
| CVE-2022-40975 | Missing Authorization vulnerability in Aazztech Post Slider.This issue affects Post Slider: from n/a through 1.6.7. | 5.4 | More Details |
| CVE-2024-3994 | The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tutor_instructor_list' shortcode in all versions up to, and including, 2.6.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 5.4 | More Details |
| CVE-2024-33680 | Cross-Site Request Forgery (CSRF) vulnerability in MainWP MainWP Child Reports.This issue affects MainWP Child Reports: from n/a through 2.1.1. | 5.4 | More Details |
| CVE-2023-20249 | A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. | 5.4 | More Details |
| CVE-2024-33632 | Cross-Site Request Forgery (CSRF) vulnerability in Piotnet Piotnet Addons For Elementor Pro.This issue affects Piotnet Addons For Elementor Pro: from n/a through 7.1.17. | 5.4 | More Details |
| CVE-2024-33682 | Cross-Site Request Forgery (CSRF) vulnerability in Cookie Information A/S WP GDPR Compliance.This issue affects WP GDPR Compliance: from n/a through 2.0.23. | 5.4 | More Details |
| CVE-2024-2404 | The Better Comments WordPress plugin before 1.5.6 does not sanitise and escape some of its settings, which could allow low privilege users such as Subscribers to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2024-4174 | Cross-Site Scripting (XSS) vulnerability in Hyperion Web Server affecting version 2.0.15. This vulnerability could allow an attacker to execute malicious Javascript code on the client by injecting that code into the URL. | 5.4 | More Details |
| CVE-2024-32812 | Server-Side Request Forgery (SSRF) vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove Podcast Publisher: from n/a through 4.0.11. | 5.4 | More Details |
| CVE-2023-6544 | A flaw was found in the Keycloak package. This issue occurs due to a permissive regular expression hardcoded for filtering which allows hosts to register a dynamic client. A malicious user with enough information about the environment could jeopardize an environment with this specific Dynamic Client Registration and TrustedDomain configuration previously unauthorized. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32808 | Authorization Bypass Through User-Controlled Key vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.9. | 5.4 | More Details |
| CVE-2024-4304 | A Cross-Site Scripting XSS vulnerability has been detected on GT3 Soluciones SWAL. This vulnerability consists in a reflected XSS in the Titular parameter inside Gestion 'Documental > Seguimiento de Expedientes > Alta de Expedientes'. | 5.4 | More Details |
| CVE-2023-47774 | Improper Restriction of Rendered UI Layers or Frames vulnerability in Automattic Jetpack allows Clickjacking.This issue affects Jetpack: from n/a before 12.7. | 5.4 | More Details |
| CVE-2024-33638 | Cross-Site Request Forgery (CSRF) vulnerability in Brijesh Kothari Smart Maintenance Mode.This issue affects Smart Maintenance Mode: from n/a through 1.4.4. | 5.4 | More Details |
| CVE-2024-28328 | CSV Injection vulnerability in the Asus RT-N12+ router allows administrator users to inject arbitrary commands or formulas in the client name parameter which can be triggered and executed in a different user session upon exporting to CSV format. | 5.4 | More Details |
| CVE-2024-4175 | Unicode transformation vulnerability in Hyperion affecting version 2.0.15. This vulnerability could allow an attacker to send a malicious payload with Unicode characters that will be replaced by ASCII characters. | 5.4 | More Details |
| CVE-2024-32793 | Cross-Site Request Forgery (CSRF) vulnerability in Paid Memberships Pro.This issue affects Paid Memberships Pro: from n/a through 2.12.10. | 5.4 | More Details |
| CVE-2024-33651 | Cross-Site Request Forgery (CSRF) vulnerability in Matthew Fries MF Gig Calendar.This issue affects MF Gig Calendar : from n/a through 1.2.1. | 5.4 | More Details |
| CVE-2024-32835 | Deserialization of Untrusted Data vulnerability in WebToffee Import Export WordPress Users.This issue affects Import Export WordPress Users: from n/a through 2.5.3. | 5.4 | More Details |
| CVE-2024-33636 | Missing Authorization vulnerability in Mahesh Vora WP Page Post Widget Clone.This issue affects WP Page Post Widget Clone: from n/a through 1.0.1. | 5.4 | More Details |
| CVE-2024-33588 | Missing Authorization vulnerability in codeSavory Knowledge Base documentation & wiki plugin – BasePress.This issue affects Knowledge Base documentation & wiki plugin – BasePress: from n/a through 2.16.1. | 5.4 | More Details |
| CVE-2023-6484 | A log injection flaw was found in Keycloak. A text string may be injected through the authentication form when using the WebAuthn authentication mode. This issue may have a minor impact to the logs integrity. | 5.3 | More Details |
| CVE-2024-32647 | Vyper is a pythonic Smart Contract Language for the Ethereum virtual machine. In versions 0.3.10 and prior, using the `create_from_blueprint` builtin can result in a double eval vulnerability when `raw_args=True` and the `args` argument has side-effects. It can be seen that the `_build_create_IR` function of the `create_from_blueprint` builtin doesn't cache the mentioned `args` argument to the stack. As such, it can be evaluated multiple times (instead of retrieving the value from the stack). No vulnerable production contracts were found. Additionally, double evaluation of side-effects should be easily discoverable in client tests. As such, the impact is low. As of time of publication, no fixed versions exist. | 5.3 | More Details |
| CVE-2024-33587 | Missing Authorization vulnerability in Copy Content Protection Team Secure Copy Content Protection and Content Locking.This issue affects Secure Copy Content Protection and Content Locking: from n/a through 3.9.0. | 5.3 | More Details |
| CVE-2024-32648 | Vyper is a pythonic Smart Contract Language for the Ethereum virtual machine. Prior to version 0.3.0, default functions don't respect nonreentrancy keys and the lock isn't emitted. No vulnerable production contracts were found. Additionally, using a lock on a `default` function is a very sparsely used pattern. As such, the impact is low. Version 0.3.0 contains a patch for the issue. | 5.3 | More Details |
| CVE-2024-32649 | Vyper is a pythonic Smart Contract Language for the Ethereum virtual machine. In versions 0.3.10 and prior, using the `sqrt` builtin can result in double eval vulnerability when the argument has side-effects. It can be seen that the `build_IR` function of the `sqrt` builtin doesn't cache the argument to the stack. As such, it can be evaluated multiple times (instead of retrieving the value from the stack). No vulnerable production contracts were found. Additionally, double evaluation of side-effects should be easily discoverable in client tests. As such, the impact is low. As of time of publication, no fixed versions are available. | 5.3 | More Details |
| CVE-2024-33586 | Missing Authorization vulnerability in Photo Gallery Team Photo Gallery by 10Web.This issue affects Photo Gallery by 10Web: from n/a through 1.8.20. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32646 | Vyper is a pythonic Smart Contract Language for the Ethereum virtual machine. In versions 0.3.10 and prior, using the `slice` builtin can result in a double eval vulnerability when the buffer argument is either `msg.data`, `self.code` or `<address>.code` and either the `start` or `length` arguments have side-effects. It can be easily triggered only with the versions `<0.3.4` as `0.3.4` introduced the unique symbol fence. No vulnerable production contracts were found. Additionally, double evaluation of side-effects should be easily discoverable in client tests. As such, the impact is low. As of time of publication, no fixed versions are available. | 5.3 | More Details |
| CVE-2024-33652 | Missing Authorization vulnerability in Real Big Plugins Client Dash.This issue affects Client Dash: from n/a through 2.2.1. | 5.3 | More Details |
| CVE-2024-32645 | Vyper is a pythonic Smart Contract Language for the Ethereum virtual machine. In versions 0.3.10 and prior, incorrect values can be logged when `raw_log` builtin is called with memory or storage arguments to be used as topics. A contract search was performed and no vulnerable contracts were found in production. The `build_IR` function of the `RawLog` class fails to properly unwrap the variables provided as topics. Consequently, incorrect values are logged as topics. As of time of publication, no fixed version is available. | 5.3 | More Details |
| CVE-2024-33596 | Missing Authorization vulnerability in Five Star Plugins Five Star Restaurant Reservations.This issue affects Five Star Restaurant Reservations: from n/a through 2.6.16. | 5.3 | More Details |
| CVE-2024-32481 | Vyper is a pythonic Smart Contract Language for the Ethereum virtual machine. Starting in version 0.3.8 and prior to version 0.4.0b1, when looping over a `range` of the form `range(start, start + N)`, if `start` is negative, the execution will always revert. This issue is caused by an incorrect assertion inserted by the code generation of the range `stmt.parse_For_range()`. The issue arises when `start` is signed, instead of using `sle`, `le` is used and `start` is interpreted as an unsigned integer for the comparison. If it is a negative number, its 255th bit is set to `1` and is hence interpreted as a very large unsigned integer making the assertion always fail. Any contract having a `range(start, start + N)` where `start` is a signed integer with the possibility for `start` to be negative is affected. If a call goes through the loop while supplying a negative `start` the execution will revert. Version 0.4.0b1 fixes the issue. | 5.3 | More Details |
| CVE-2024-32676 | Improper Restriction of Excessive Authentication Attempts vulnerability in LoginPress LoginPress Pro allows Removing Important Client Functionality.This issue affects LoginPress Pro: from n/a before 3.0.0. | 5.3 | More Details |
| CVE-2024-33538 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Fastline Media LLC Assistant – Every Day Productivity Apps.This issue affects Assistant – Every Day Productivity Apps: from n/a through 1.4.9.1. | 5.3 | More Details |
| CVE-2024-33575 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in User Meta user-meta.This issue affects User Meta: from n/a through 3.0. | 5.3 | More Details |
| CVE-2024-0874 | A flaw was found in coredns. This issue could lead to invalid cache entries returning due to incorrectly implemented caching. | 5.3 | More Details |
| CVE-2024-1726 | A flaw was discovered in the RESTEasy Reactive implementation in Quarkus. Due to security checks for some JAX-RS endpoints being performed after serialization, more processing resources are consumed while the HTTP request is checked. In certain configurations, if an attacker has knowledge of any POST, PUT, or PATCH request paths, they can potentially identify vulnerable endpoints and trigger excessive resource usage as the endpoints process the requests. This can result in a denial of service. | 5.3 | More Details |
| CVE-2024-29660 | Cross Site Scripting vulnerability in DedeCMS v.5.7 allows a local attacker to execute arbitrary code via a crafted payload to the stepselect_main.php component. | 5.3 | More Details |
| CVE-2024-3733 | The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.9.15 via the ajax_load_more() , eael_woo_pagination_product_ajax(), and ajax_eael_product_gallery() functions. This makes it possible for unauthenticated attackers to extract posts that may be in private or draft status. | 5.3 | More Details |
| CVE-2023-23989 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss RegistrationMagic.This issue affects RegistrationMagic: from n/a through 5.1.9.2. | 5.3 | More Details |
| CVE-2023-50432 | simple-dhcp-server through ec976d2 allows remote attackers to cause a denial of service (daemon crash) by sending a DHCP packet without any option fields, which causes free_packet in dhcp_packet.c to dereference a NULL pointer. | 5.3 | More Details |
| CVE-2024-32826 | Missing Authorization vulnerability in Vektor,Inc. VK Block Patterns.This issue affects VK Block Patterns: from n/a through 1.31.0. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-48763 | Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS vulnerability in Crocoblock JetFormBuilder allows Code Injection.This issue affects JetFormBuilder: from n/a through 3.1.4. | 5.3 | More Details |
| CVE-2024-34044 | The O-RAN E2T I-Release buildPrometheusList function can have a NULL pointer dereference because peerInfo can be NULL. | 5.3 | More Details |
| CVE-2024-34043 | O-RAN RICAPP kpimon-go I-Release has a segmentation violation via a certain E2AP-PDU message. | 5.3 | More Details |
| CVE-2023-51405 | Improper Authentication vulnerability in Repute Infosystems BookingPress allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects BookingPress: from n/a through 1.0.74. | 5.3 | More Details |
| CVE-2024-32678 | Missing Authorization vulnerability in TrackShip TrackShip for WooCommerce.This issue affects TrackShip for WooCommerce: from n/a through 1.7.5. | 5.3 | More Details |
| CVE-2022-48634 | In the Linux kernel, the following vulnerability has been resolved: drm/gma500: Fix BUG: sleeping function called from invalid context errors gma_crtc_page_flip() was holding the event_lock spinlock while calling crtc_funcs->mode_set_base() which takes ww_mutex. The only reason to hold event_lock is to clear gma_crtc->page_flip_event on mode_set_base() errors. Instead unlock it after setting gma_crtc->page_flip_event and on errors re-take the lock and clear gma_crtc->page_flip_event it it is still set. This fixes the following WARN/stacktrace: [ 512.122953] BUG: sleeping function called from invalid context at kernel/locking/mutex.c:870 [ 512.123004] in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 1253, name: gnome-shell [ 512.123031] preempt_count: 1, expected: 0 [ 512.123048] RCU nest depth: 0, expected: 0 [ 512.123066] INFO: lockdep is turned off. [ 512.123080] irq event stamp: 0 [ 512.123094] hardirqs last enabled at (0): [<0000000000000000>] 0x0 [ 512.123134] hardirqs last disabled at (0): [<ffffffff8d0ec28c>] copy_process+0x9fc/0x1de0 [ 512.123176] softirqs last enabled at (0): [<ffffffff8d0ec28c>] copy_process+0x9fc/0x1de0 [ 512.123207] softirqs last disabled at (0): [<0000000000000000>] 0x0 [ 512.123233] Preemption disabled at: [ 512.123241] [<0000000000000000>] 0x0 [ 512.123275] CPU: 3 PID: 1253 Comm: gnome-shell Tainted: G W 5.19.0+ #1 [ 512.123304] Hardware name: Packard Bell dot s/SJE01_CT, BIOS V1.10 07/23/2013 [ 512.123323] Call Trace: [ 512.123346] <TASK> [ 512.123370] dump_stack_lvl+0x5b/0x77 [ 512.123412] __might_resched.cold+0xff/0x13a [ 512.123458] ww_mutex_lock+0x1e/0xa0 [ 512.123495] psb_gem_pin+0x2c/0x150 [gma500_gfx] [ 512.123601] gma_pipe_set_base+0x76/0x240 [gma500_gfx] [ 512.123708] gma_crtc_page_flip+0x95/0x130 [gma500_gfx] [ 512.123808] drm_mode_page_flip_ioctl+0x57d/0x5d0 [ 512.123897] ? drm_mode_cursor2_ioctl+0x10/0x10 [ 512.123936] drm_ioctl_kernel+0xa1/0x150 [ 512.123984] drm_ioctl+0x21f/0x420 [ 512.124025] ? drm_mode_cursor2_ioctl+0x10/0x10 [ 512.124070] ? rcu_read_lock_bh_held+0xb/0x60 [ 512.124104] ? lock_release+0x1ef/0x2d0 [ 512.124161] __x64_sys_ioctl+0x8d/0xd0 [ 512.124203] do_syscall_64+0x58/0x80 [ 512.124239] ? do_syscall_64+0x67/0x80 [ 512.124267] ? trace_hardirqs_on_prepare+0x55/0xe0 [ 512.124300] ? do_syscall_64+0x67/0x80 [ 512.124340] ? rcu_read_lock_sched_held+0x10/0x80 [ 512.124377] entry_SYSCALL_64_after_hwframe+0x63/0xcd [ 512.124411] RIP: 0033:0x7fcc4a70740f [ 512.124442] Code: 00 48 89 44 24 18 31 c0 48 8d 44 24 60 c7 04 24 10 00 00 00 48 89 44 24 08 48 8d 44 24 20 48 89 44 24 10 b8 10 00 00 00 0f 05 <89> c2 3d 00 f0 ff ff 77 18 48 8b 44 24 18 64 48 2b 04 25 28 00 00 [ 512.124470] RSP: 002b:00007ffda73f5390 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [ 512.124503] RAX: ffffffffffffffda RBX: 000055cc9e474500 RCX: 00007fcc4a70740f [ 512.124524] RDX: 00007ffda73f5420 RSI: 00000000c01864b0 RDI: 0000000000000009 [ 512.124544] RBP: 00007ffda73f5420 R08: 000055cc9c0b0cb0 R09: 0000000000000034 [ 512.124564] R10: 0000000000000000 R11: 0000000000000246 R12: 00000000c01864b0 [ 512.124584] R13: 0000000000000009 R14: 000055cc9df484d0 R15: 000055cc9af5d0c0 [ 512.124647] </TASK> | 5.3 | More Details |
| CVE-2024-3893 | The Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the rtcl_fb_gallery_image_delete AJAX action in all versions up to, and including, 3.0.10.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary attachements. | 5.3 | More Details |
| CVE-2024-32788 | Insertion of Sensitive Information into Log File vulnerability in Frédéric GILLES FG Joomla to WordPress.This issue affects FG Joomla to WordPress: from n/a through 4.20.2. | 5.3 | More Details |
| CVE-2023-32127 | Missing Authorization vulnerability in Daniel Powney Multi Rating allows Functionality Misuse.This issue affects Multi Rating: from n/a through 5.0.6. | 5.3 | More Details |
| CVE-2024-2920 | The WP-Members Membership Plugin plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 3.4.9.3 due to the plugin uploading user supplied files to a publicly accessible directory in wp-content without any restrictions. This makes it possible for unauthenticated attackers to view files uploaded by other users which may contain sensitive information. | 5.3 | More Details |
| CVE-2024-3682 | The WP STAGING and WP STAGING Pro plugins for WordPress are vulnerable to Sensitive Information Exposure in versions up to, and including, 3.4.3, and versions up to, and including, 5.4.3, respectively, via the ajaxSendReport function. This makes it possible for unauthenticated attackers to extract sensitive data from a log file, including system information and (in the Pro version) license keys. Successful exploitation requires an administrator to have used the 'Contact Us' functionality along with the "Enable this option to automatically submit the log files." option. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3678 | The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.4.2. This makes it possible for unauthenticated attackers to view limited information from password protected posts. | 5.3 | More Details |
| CVE-2024-32716 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StreamWeasels StreamWeasels Twitch Integration.This issue affects StreamWeasels Twitch Integration: from n/a through 1.7.8. | 5.3 | More Details |
| CVE-2024-33664 | python-jose through 3.3.0 allows attackers to cause a denial of service (resource consumption) during a decode via a crafted JSON Web Encryption (JWE) token with a high compression ratio, aka a "JWT bomb." This is similar to CVE-2024-21319. | 5.3 | More Details |
| CVE-2023-25785 | Missing Authorization vulnerability in Shoaib Saleem WP Post Rating allows Functionality Misuse.This issue affects WP Post Rating: from n/a through 2.5. | 5.3 | More Details |
| CVE-2022-48638 | In the Linux kernel, the following vulnerability has been resolved: cgroup: cgroup_get_from_id() must check the looked-up kn is a directory cgroup has to be one kernfs dir, otherwise kernel panic is caused, especially cgroup id is provide from userspace. | 5.3 | More Details |
| CVE-2024-32823 | Authorization Bypass Through User-Controlled Key vulnerability in FeedbackWP Rate my Post – WP Rating System.This issue affects Rate my Post – WP Rating System: from n/a through 3.4.4. | 5.3 | More Details |
| CVE-2023-25790 | Improper Authentication, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xtemos WoodMart allows Cross-Site Scripting (XSS).This issue affects WoodMart: from n/a through 7.0.4. | 5.3 | More Details |
| CVE-2023-50059 | An issue ingalxe.com Galxe platform 1.0 allows a remote attacker to obtain sensitive information via the Web3 authentication process of Galxe, the signed message lacks a nonce (random number) | 5.3 | More Details |
| CVE-2024-33260 | Jerryscript commit cefd391 was discovered to contain a segmentation violation via the component parser_parse_class at jerry-core/parser/js/js-parser-expr.c | 5.1 | More Details |
| CVE-2023-38002 | IBM Storage Scale 5.1.0.0 through 5.1.9.2 could allow an authenticated user to steal or manipulate an active session to gain access to the system. IBM X-Force ID: 260208. | 5.0 | More Details |
| CVE-2023-3597 | A flaw was found in Keycloak, where it does not correctly validate its client step-up authentication in org.keycloak.authentication. This flaw allows a remote user authenticated with a password to register a false second authentication factor along with an existing one and bypass authentication. | 5.0 | More Details |
| CVE-2024-33590 | Server-Side Request Forgery (SSRF) vulnerability in codeSavory Knowledge Base documentation & wiki plugin – BasePress.This issue affects Knowledge Base documentation & wiki plugin – BasePress: from n/a through 2.16.1. | 5.0 | More Details |
| CVE-2023-50361 | A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later | 5.0 | More Details |
| CVE-2023-50362 | A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.6.2722 build 20240402 and later QuTS hero h5.1.6.2734 build 20240414 and later | 5.0 | More Details |
| CVE-2024-31574 | Cross Site Scripting vulnerability in TWCMS v.2.6 allows a local attacker to execute arbitrary code via a crafted script | 5.0 | More Details |
| CVE-2024-32819 | Server-Side Request Forgery (SSRF) vulnerability in Culqi.This issue affects Culqi: from n/a through 3.0.14. | 4.9 | More Details |
| CVE-2024-32879 | Python Social Auth is a social authentication/registration mechanism. Prior to version 5.4.1, due to default case-insensitive collation in MySQL or MariaDB databases, third-party authentication user IDs are not case-sensitive and could cause different IDs to match. This issue has been addressed by a fix released in version 5.4.1. An immediate workaround would be to change collation of the affected field. | 4.9 | More Details |
| CVE-2024-32955 | Server-Side Request Forgery (SSRF) vulnerability in Foliovision FV Flowplayer Video Player.This issue affects FV Flowplayer Video Player: from n/a through 7.5.43.7212. | 4.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32718 | Server-Side Request Forgery (SSRF) vulnerability in Webangon The Pack Elementor.This issue affects The Pack Elementor addons: from n/a through 2.0.8.2. | 4.9 | More Details |
| CVE-2024-4296 | The account management interface of HGiga iSherlock (including MailSherlock, SpamSherlock, AuditSherlock) fails to filter special characters in certain function parameters, allowing remote attackers with administrative privileges to exploit this vulnerability to download arbitrary system files. | 4.9 | More Details |
| CVE-2024-32775 | Server-Side Request Forgery (SSRF) vulnerability in Pavex Embed Google Photos album.This issue affects Embed Google Photos album: from n/a through 2.1.9. | 4.9 | More Details |
| CVE-2024-4297 | The system configuration interface of HGiga iSherlock (including MailSherlock, SpamSherlock, AuditSherlock) fails to filter special characters in certain function parameters, allowing remote attackers with administrative privileges to exploit this vulnerability to download arbitrary system files. | 4.9 | More Details |
| CVE-2024-3261 | The Strong Testimonials WordPress plugin before 3.1.12 does not validate and escape some of its Testimonial fields before outputting them back in a page/post, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. The attack requires a specific view to be performed | 4.8 | More Details |
| CVE-2024-30890 | Cross Site Scripting vulnerability in ED01-CMS v.1.0 allows an attacker to obtain sensitive information via the categories.php component. | 4.7 | More Details |
| CVE-2024-33584 | URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Deepen Bajracharya Video Conferencing with Zoom.This issue affects Video Conferencing with Zoom: from n/a through 4.4.4. | 4.7 | More Details |
| CVE-2024-4255 | A vulnerability, which was classified as critical, has been found in Ruijie RG-UAC up to 20240419. This issue affects some unknown processing of the file /view/network Config/GRE/gre_edit_commit.php. The manipulation of the argument 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 identifier VDB-262145 was assigned to this vulnerability. | 4.7 | More Details |
| CVE-2022-48650 | In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix memory leak in __qlt_24xx_handle_abts() Commit 8f394da36a36 ("scsi: qla2xxx: Drop TARGET_SCF_LOOKUP_LUN_FROM_TAG") made the __qlt_24xx_handle_abts() function return early if tcm_qla2xxx_find_cmd_by_tag() didn't find a command, but it missed to clean up the allocated memory for the management command. | 4.7 | More Details |
| CVE-2024-3195 | A vulnerability was found in MailCleaner up to 2023.03.14. It has been classified as critical. This affects an unknown part of the component Admin Endpoints. 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. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-262311. | 4.7 | More Details |
| CVE-2024-32957 | Missing Authorization vulnerability in Live Composer Team Page Builder: Live Composer.This issue affects Page Builder: Live Composer: from n/a through 1.5.38. | 4.7 | More Details |
| CVE-2024-2159 | The Social Sharing Plugin WordPress plugin before 3.3.61 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 4.7 | More Details |
| CVE-2024-3265 | The Advanced Search WordPress plugin through 1.1.6 does not properly escape parameters appended to an SQL query, making it possible for users with the administrator role to conduct SQL Injection attacks in the context of a multisite WordPress configurations. | 4.7 | More Details |
| CVE-2024-33905 | In Telegram WebK before 2.0.0 (488), a crafted Mini Web App allows XSS via the postMessage web_app_open_link event type. | 4.6 | More Details |
| CVE-2024-3060 | The ENL Newsletter WordPress plugin through 1.0.1 does not sanitize and escape a parameter before using it in a SQL statement, allowing admin+ to perform SQL injection attacks | 4.5 | More Details |
| CVE-2024-32817 | Deserialization of Untrusted Data vulnerability in Import and export users and customers.This issue affects Import and export users and customers: from n/a through 1.26.2. | 4.4 | More Details |
| CVE-2024-33627 | Server-Side Request Forgery (SSRF) vulnerability in Cusmin Absolutely Glamorous Custom Admin.This issue affects Absolutely Glamorous Custom Admin: from n/a through 7.2.2. | 4.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-2258 | The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a user's display name autofilled into forms in all versions up to, and including, 1.15.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 4.4 | More Details |
| CVE-2024-33629 | Server-Side Request Forgery (SSRF) vulnerability in Creative Motion Auto Featured Image (Auto Post Thumbnail).This issue affects Auto Featured Image (Auto Post Thumbnail): from n/a through 4.0.0. | 4.4 | More Details |
| CVE-2024-4006 | An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.7 before 16.9.6, all versions starting from 16.10 before 16.10.4, all versions starting from 16.11 before 16.11.1 where personal access scopes were not honored by GraphQL subscriptions | 4.3 | More Details |
| CVE-2024-32046 | Mattermost versions 9.6.x <= 9.6.0, 9.5.x <= 9.5.2, 9.4.x <= 9.4.4 and 8.1.x <= 8.1.11 fail to remove detailed error messages in API requests even if the developer mode is off which allows an attacker to get information about the server such as the full path were files are stored | 4.3 | More Details |
| CVE-2024-33851 | phpecc, as used in paragonie/phpecc before 2.0.1, has a branch-based timing leak in Point addition. (This is related to phpecc/phpecc on GitHub, and the Matyas Danter ECC library.) | 4.3 | More Details |
| CVE-2024-33650 | Cross-Site Request Forgery (CSRF) vulnerability in Cryout Creations Serious Slider.This issue affects Serious Slider: from n/a through 1.2.4. | 4.3 | More Details |
| CVE-2024-32772 | Authorization Bypass Through User-Controlled Key vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.9. | 4.3 | More Details |
| CVE-2024-32699 | Cross-Site Request Forgery (CSRF) vulnerability in YITH YITH WooCommerce Compare.This issue affects YITH WooCommerce Compare: from n/a through 2.37.0. | 4.3 | More Details |
| CVE-2024-32728 | Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs Paid Member Subscriptions.This issue affects Paid Member Subscriptions: from n/a through 2.11.0. | 4.3 | More Details |
| CVE-2024-32796 | Insertion of Sensitive Information into Log File vulnerability in Very Good Plugins WP Fusion Lite.This issue affects WP Fusion Lite: from n/a through 3.42.10. | 4.3 | More Details |
| CVE-2024-32773 | Cross-Site Request Forgery (CSRF) vulnerability in WP Royal Royal Elementor Kit.This issue affects Royal Elementor Kit: from n/a through 1.0.116. | 4.3 | More Details |
| CVE-2024-3072 | The ACF Front End Editor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_texts() function in all versions up to, and including, 2.0.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to update arbitrary post title, content, and ACF data. | 4.3 | More Details |
| CVE-2024-32795 | Cross-Site Request Forgery (CSRF) vulnerability in Revmakx WPCal.Io – Easy Meeting Scheduler.This issue affects WPCal.Io – Easy Meeting Scheduler: from n/a through 0.9.5.8. | 4.3 | More Details |
| CVE-2024-32806 | Cross-Site Request Forgery (CSRF) vulnerability in CoSchedule Headline Analyzer.This issue affects Headline Analyzer: from n/a through 1.3.3. | 4.3 | More Details |
| CVE-2024-32947 | Cross-Site Request Forgery (CSRF) vulnerability in AlumniOnline Web Services LLC WP ADA Compliance Check Basic.This issue affects WP ADA Compliance Check Basic: from n/a through 3.1.3. | 4.3 | More Details |
| CVE-2024-34047 | O-RAN RIC I-Release e2mgr lacks array size checks in RicServiceUpdateHandler. | 4.3 | More Details |
| CVE-2024-4182 | Mattermost versions 9.6.0, 9.5.x before 9.5.3, 9.4.x before 9.4.5, and 8.1.x before 8.1.12 fail to handle JSON parsing errors in custom status values, which allows an authenticated attacker to crash other users' web clients via a malformed custom status. | 4.3 | More Details |
| CVE-2024-4183 | Mattermost versions 8.1.x before 8.1.12, 9.6.x before 9.6.1, 9.5.x before 9.5.3, 9.4.x before 9.4.5 fail to limit the number of active sessions, which allows an authenticated attacker to crash the server via repeated requests to the getSessions API after flooding the sessions table. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32782 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in HasThemes HT Mega.This issue affects HT Mega: from n/a through 2.4.7. | 4.3 | More Details |
| CVE-2024-2908 | The Call Now Button WordPress plugin before 1.4.7 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). | 4.3 | More Details |
| CVE-2024-32828 | Missing Authorization vulnerability in Octolize Flexible Shipping.This issue affects Flexible Shipping: from n/a through 4.24.15. | 4.3 | More Details |
| CVE-2024-32829 | Missing Authorization vulnerability in Supsystic Data Tables Generator by Supsystic.This issue affects Data Tables Generator by Supsystic: from n/a through 1.10.31. | 4.3 | More Details |
| CVE-2024-33677 | Cross-Site Request Forgery (CSRF) vulnerability in Renzo Johnson Contact Form 7 Extension For Mailchimp.This issue affects Contact Form 7 Extension For Mailchimp: from n/a through 0.5.70. | 4.3 | More Details |
| CVE-2024-33678 | Cross-Site Request Forgery (CSRF) vulnerability in ClickCease ClickCease Click Fraud Protection.This issue affects ClickCease Click Fraud Protection: from n/a through 3.2.4. | 4.3 | More Details |
| CVE-2024-33679 | Cross-Site Request Forgery (CSRF) vulnerability in FameThemes FameTheme Demo Importer.This issue affects FameTheme Demo Importer: from n/a through 1.1.5. | 4.3 | More Details |
| CVE-2024-33683 | Cross-Site Request Forgery (CSRF) vulnerability in WP Republic Hide Dashboard Notifications.This issue affects Hide Dashboard Notifications: from n/a through 1.2.3. | 4.3 | More Details |
| CVE-2024-32822 | Missing Authorization vulnerability in impleCode Reviews Plus.This issue affects Reviews Plus: from n/a through 1.3.4. | 4.3 | More Details |
| CVE-2024-33688 | Cross-Site Request Forgery (CSRF) vulnerability in Extend Themes Teluro.This issue affects Teluro: from n/a through 1.0.31. | 4.3 | More Details |
| CVE-2024-33689 | Cross-Site Request Forgery (CSRF) vulnerability in Tony Zeoli, Tony Hayes Radio Station.This issue affects Radio Station: from n/a through 2.5.7. | 4.3 | More Details |
| CVE-2024-33690 | Cross-Site Request Forgery (CSRF) vulnerability in Jegstudio Financio.This issue affects Financio: from n/a through 1.1.3. | 4.3 | More Details |
| CVE-2024-33691 | Cross-Site Request Forgery (CSRF) vulnerability in OptinMonster Popup Builder Team OptinMonster.This issue affects OptinMonster: from n/a through 2.15.3. | 4.3 | More Details |
| CVE-2024-4348 | A vulnerability, which was classified as problematic, was found in osCommerce 4. Affected is an unknown function of the file /catalog/all-products. The manipulation of the argument cat 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-262488. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 4.3 | More Details |
| CVE-2024-32432 | Missing Authorization vulnerability in Ovic Team Ovic Addon Toolkit.This issue affects Ovic Addon Toolkit: from n/a through 2.6.1. | 4.3 | More Details |
| CVE-2024-32794 | Cross-Site Request Forgery (CSRF) vulnerability in Paid Memberships Pro.This issue affects Paid Memberships Pro: from n/a through 2.12.10. | 4.3 | More Details |
| CVE-2024-33542 | Authorization Bypass Through User-Controlled Key vulnerability in Fabio Rinaldi Crelly Slider.This issue affects Crelly Slider: from n/a through 1.4.5. | 4.3 | More Details |
| CVE-2024-33585 | Missing Authorization vulnerability in Tyche Softwares Payment Gateway Based Fees and Discounts for WooCommerce.This issue affects Payment Gateway Based Fees and Discounts for WooCommerce: from n/a through 2.12.1. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-1347 | An issue has been discovered in GitLab CE/EE affecting all versions before 16.9.6, all versions starting from 16.10 before 16.10.4, all versions starting from 16.11 before 16.11.1. Under certain conditions, an attacker through a crafted email address may be able to bypass domain based restrictions on an instance or a group. | 4.3 | More Details |
| CVE-2024-3194 | A vulnerability was found in MailCleaner up to 2023.03.14 and classified as problematic. Affected by this issue is some unknown functionality of the component Log File Endpoint. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-262310 is the identifier assigned to this vulnerability. | 4.3 | More Details |
| CVE-2024-33593 | Missing Authorization vulnerability in RedNao Smart Forms.This issue affects Smart Forms: from n/a through 2.6.91. | 4.3 | More Details |
| CVE-2024-3508 | A flaw was found in Bombastic, which allows authenticated users to upload compressed (bzip2 or zstd) SBOMs. The API endpoint verifies the presence of some fields and values in the JSON. To perform this verification, the uploaded file must first be decompressed. | 4.3 | More Details |
| CVE-2024-33670 | Passbolt API before 4.6.2 allows HTML injection in a URL parameter, resulting in custom content being displayed when a user visits the crafted URL. Although the injected content is not executed as JavaScript due to Content Security Policy (CSP) restrictions, it may still impact the appearance and user interaction of the page. | 4.3 | More Details |
| CVE-2024-33595 | Missing Authorization vulnerability in Jewel Theme Master Addons for Elementor.This issue affects Master Addons for Elementor: from n/a through 2.0.5.4.1. | 4.3 | More Details |
| CVE-2024-2429 | The Salon booking system WordPress plugin through 9.6.5 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack | 4.3 | More Details |
| CVE-2024-33686 | Missing Authorization vulnerability in Extend Themes Pathway, Extend Themes Hugo WP, Extend Themes Althea WP, Extend Themes Elevate WP, Extend Themes Brite, Extend Themes Colibri WP, Extend Themes Vertice.This issue affects Pathway: from n/a through 1.0.15; Hugo WP: from n/a through 1.0.8; Althea WP: from n/a through 1.0.13; Elevate WP: from n/a through 1.0.15; Brite: from n/a through 1.0.11; Colibri WP: from n/a through 1.0.94; Vertice: from n/a through 1.0.7. | 4.3 | More Details |
| CVE-2024-4159 | Brocade SANnav before v2.3.0a lacks protection mechanisms on port 2377/TCP and 7946/TCP, which could allow an unauthenticated attacker to sniff the SANnav Docker information. | 4.3 | More Details |
| CVE-2024-3192 | A vulnerability, which was classified as problematic, was found in MailCleaner up to 2023.03.14. Affected is an unknown function of the component Admin Interface. The manipulation as part of Mail Message 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. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-262308. | 4.3 | More Details |
| CVE-2023-52220 | Missing Authorization vulnerability in MonsterInsights Google Analytics by Monster Insights.This issue affects Google Analytics by Monster Insights: from n/a through 8.21.0. | 4.3 | More Details |
| CVE-2024-4172 | A vulnerability classified as problematic was found in idcCMS 1.35. Affected by this vulnerability is an unknown functionality of the file /admin/admin_cl.php?mudi=revPwd. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-261991. | 4.3 | More Details |
| CVE-2023-51710 | EMS SQL Manager 3.6.2 (build 55333) for Oracle allows DLL hijacking: a user can trigger the execution of arbitrary code every time the product is executed. | 4.2 | More Details |
| CVE-2023-41290 | A path traversal vulnerability has been reported to affect QuFirewall. If exploited, the vulnerability could allow authenticated administrators to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following version: QuFirewall 2.4.1 ( 2024/02/01 ) and later | 4.1 | More Details |
| CVE-2024-32078 | URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Foliovision FV Flowplayer Video Player.This issue affects FV Flowplayer Video Player: from n/a through 7.5.44.7212. | 4.1 | More Details |
| CVE-2024-33883 | The ejs (aka Embedded JavaScript templates) package before 3.1.10 for Node.js lacks certain pollution protection. | 4.0 | More Details |
| CVE-2024-3076 | The MM-email2image WordPress plugin through 0.2.5 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 | 3.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-23985 | Missing Authorization vulnerability in Quiz Maker team Quiz Maker.This issue affects Quiz Maker: from n/a through 6.3.9.4. | 3.7 | More Details |
| CVE-2024-32236 | An issue in CmsEasy v.7.7 and before allows a remote attacker to obtain sensitive information via the update function in the index.php component. | 3.5 | More Details |
| CVE-2024-4327 | A vulnerability was found in Apryse WebViewer up to 10.8.0. It has been classified as problematic. This affects an unknown part of the component PDF Document Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 10.9 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-262419. NOTE: The vendor was contacted early about this disclosure and explains that the documentation recommends a strict Content Security Policy and the issue was fixed in release 10.9. | 3.5 | More Details |
| CVE-2024-4226 | It was identified that in certain versions of Octopus Server, that a user created with no permissions could view all users, user roles and permissions. This functionality was removed in versions of Octopus Server after the fixed versions listed. | 3.5 | More Details |
| CVE-2024-4293 | A vulnerability classified as problematic was found in PHPGurukul Doctor Appointment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file appointment-bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-262225 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2024-28977 | Dell Repository Manager, versions 3.4.2 through 3.4.4,contains a Path Traversal vulnerability in logger module. A local attacker with low privileges could potentially exploit this vulnerability to gain unauthorized read access to the files stored on the server filesystem with the privileges of the running web application. | 3.3 | More Details |
| CVE-2024-23228 | This issue was addressed through improved state management. This issue is fixed in iOS 17.3 and iPadOS 17.3. Locked Notes content may have been unexpectedly unlocked. | 3.3 | More Details |
| CVE-2024-22091 | Mattermost versions 8.1.x <= 8.1.10, 9.6.x <= 9.6.0, 9.5.x <= 9.5.2 and 8.1.x <= 8.1.11 fail to limit the size of a request path that includes user inputs which allows an attacker to cause excessive resource consumption, possibly leading to a DoS via sending large request paths | 3.1 | More Details |
| CVE-2024-4141 | Out-of-bounds array write in Xpdf 4.05 and earlier, triggered by an invalid character code in a Type 1 font. The root problem was a bounds check that was being optimized away by modern compilers. | 2.9 | More Details |
| CVE-2024-3034 | The BackUpWordPress plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.13 via the hmbkp_directory_browse parameter. This makes it possible for authenticated attackers, with administrator-level access and above, to traverse directories outside of the context in which the plugin should allow. | 2.7 | More Details |
| CVE-2024-4198 | Mattermost versions 9.6.0, 9.5.x before 9.5.3, and 8.1.x before 8.1.12 fail to fully validate role changes which allows an attacker authenticated as team admin to demote users to guest via crafted HTTP requests. | 2.7 | More Details |
| CVE-2024-4235 | A vulnerability classified as problematic was found in Netgear DG834Gv5 1.6.01.34. This vulnerability affects unknown code of the component Web Management Interface. The manipulation leads to cleartext storage of sensitive information. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-262126 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 2.7 | More Details |
| CVE-2024-4195 | Mattermost versions 9.6.0, 9.5.x before 9.5.3, and 8.1.x before 8.1.12 fail to fully validate role changes, which allows an attacker authenticated as a team admin to promote guests to team admins via crafted HTTP requests. | 2.7 | More Details |
| CVE-2024-4256 | A vulnerability was found in Techkshetra Info Solutions Savsoft Quiz 6.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /public/index.php/Qbank/editCategory of the component Category Page. The manipulation of the argument category_name with the input ><script>alert('XSS')</script> 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-262148. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 2.4 | More Details |
| CVE-2024-31747 | An issue in Yealink VP59 Microsoft Teams Phone firmware 91.15.0.118 (fixed in 122.15.0.142) allows a physically proximate attacker to disable the phone lock via the Walkie Talkie menu option. | 2.1 | More Details |
| CVE-2019-19752 | nvOC through 3.2 ships with SSH host keys baked into the installation image, which allows man-in-the-middle attacks and makes identification of all public IPv4 nodes trivial with Shodan.io. NOTE: as of 2019-12-01, the vendor indicated plans to fix this in the next image build. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2019-19751 | easyMINE before 2019-12-05 ships with SSH host keys baked into the installation image, which allows man-in-the-middle attacks and makes identification of all public IPv4 nodes trivial with Shodan.io. | N/A | More Details |
| CVE-2024-2439 | The Salon booking system WordPress plugin through 9.6.5 does not sanitise and escape some of its settings, which could allow high privilege users such as Editor 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-2023-36268 | Rejected reason: DoS issues, or unexploitable crashes, are out of scope for vulnerabilities. | N/A | More Details |
| CVE-2024-34011 | Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 37758. | N/A | More Details |
| CVE-2024-32268 | An issue in Tuya Smart camera U6N v.3.2.5 allows a remote attacker to cause a denial of service via a crafted packet to the network connection component. | N/A | More Details |
| CVE-2023-52646 | In the Linux kernel, the following vulnerability has been resolved: aio: fix mremap after fork null-deref Commit e4a0d3e720e7 ("aio: Make it possible to remap aio ring") introduced a null-deref if mremap is called on an old aio mapping after fork as mm->ioctx_table will be set to NULL. [jmoyer@redhat.com: fix 80 column issue] | N/A | More Details |
| CVE-2023-48684 | Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 37758. | N/A | More Details |
| CVE-2024-2972 | The Floating Chat Widget: Contact Chat Icons, WhatsApp, Telegram Chat, Line Messenger, WeChat, Email, SMS, Call Button WordPress plugin before 3.1.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | N/A | More Details |
| CVE-2024-33332 | An issue discovered in SpringBlade 3.7.1 allows attackers to obtain sensitive information via crafted GET request to api/blade-system/tenant. | N/A | More Details |
| CVE-2023-48683 | Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 37758, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 39169. | N/A | More Details |
| CVE-2023-46270 | MacPaw The Unarchiver before 4.3.6 contains vulnerability related to missing quarantine attributes for extracted items. | N/A | More Details |
| CVE-2024-33436 | An issue in CSS Exfil Protection v.1.1.0 allows a remote attacker to obtain sensitive information due to missing support for CSS variables | N/A | More Details |
| CVE-2024-29466 | Directory Traversal vulnerability in lsgwr spring boot online exam v.0.9 allows an attacker to execute arbitrary code via the FileTransUtil.java component. | N/A | More Details |
| CVE-2024-1756 | The WooCommerce Customers Manager WordPress plugin before 29.8 does not have authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber, to call it and retrieve the list of customer email addresses along with their id, first name and last name | N/A | More Details |
| CVE-2024-34010 | Local privilege escalation due to unquoted search path vulnerability. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 37758, Acronis Cyber Protect 16 (Windows) before build 38690. | N/A | More Details |
| CVE-2022-48632 | In the Linux kernel, the following vulnerability has been resolved: i2c: mlxbf: prevent stack overflow in mlxbf_i2c_smbus_start_transaction() memcpy() is called in a loop while 'operation->length' upper bound is not checked and 'data_idx' also increments. | N/A | More Details |
| CVE-2024-1905 | The Smart Forms WordPress plugin before 2.6.96 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 Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2022-48664 | In the Linux kernel, the following vulnerability has been resolved: btrfs: fix hang during unmount when stopping a space reclaim worker Often when running generic/562 from fstests we can hang during unmount, resulting in a trace like this: Sep 07 11:52:00 debian9 unknown: run fstests generic/562 at 2022-09-07 11:52:00 Sep 07 11:55:32 debian9 kernel: INFO: task umount:49438 blocked for more than 120 seconds. Sep 07 11:55:32 debian9 kernel: Not tainted 6.0.0-rc2-btrfs-next-122 #1 Sep 07 11:55:32 debian9 kernel: "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. Sep 07 11:55:32 debian9 kernel: task:umount state:D stack: 0 pid:49438 ppid: 25683 flags:0x00004000 Sep 07 11:55:32 debian9 kernel: Call Trace: Sep 07 11:55:32 debian9 kernel: <TASK> Sep 07 11:55:32 debian9 kernel: __schedule+0x3c8/0xec0 Sep 07 11:55:32 debian9 kernel: ? rcu_read_lock_sched_held+0x12/0x70 Sep 07 11:55:32 debian9 kernel: schedule+0x5d/0xf0 Sep 07 11:55:32 debian9 kernel: schedule_timeout+0xf1/0x130 Sep 07 11:55:32 debian9 kernel: ? lock_release+0x224/0x4a0 Sep 07 11:55:32 debian9 kernel: ? lock_acquired+0x1a0/0x420 Sep 07 11:55:32 debian9 kernel: ? trace_hardirqs_on+0x2c/0xd0 Sep 07 11:55:32 debian9 kernel: __wait_for_common+0xac/0x200 Sep 07 11:55:32 debian9 kernel: ? usleep_range_state+0xb0/0xb0 Sep 07 11:55:32 debian9 kernel: __flush_work+0x26d/0x530 Sep 07 11:55:32 debian9 kernel: ? flush_workqueue_prep_pwqs+0x140/0x140 Sep 07 11:55:32 debian9 kernel: ? trace_clock_local+0xc/0x30 Sep 07 11:55:32 debian9 kernel: __cancel_work_timer+0x11f/0x1b0 Sep 07 11:55:32 debian9 kernel: ? close_ctree+0x12b/0x5b3 [btrfs] Sep 07 11:55:32 debian9 kernel: ? __trace_bputs+0x10b/0x170 Sep 07 11:55:32 debian9 kernel: close_ctree+0x152/0x5b3 [btrfs] Sep 07 11:55:32 debian9 kernel: ? evict_inodes+0x166/0x1c0 Sep 07 11:55:32 debian9 kernel: generic_shutdown_super+0x71/0x120 Sep 07 11:55:32 debian9 kernel: kill_anon_super+0x14/0x30 Sep 07 11:55:32 debian9 kernel: btrfs_kill_super+0x12/0x20 [btrfs] Sep 07 11:55:32 debian9 kernel: deactivate_locked_super+0x2e/0xa0 Sep 07 11:55:32 debian9 kernel: cleanup_mnt+0x100/0x160 Sep 07 11:55:32 debian9 kernel: task_work_run+0x59/0xa0 Sep 07 11:55:32 debian9 kernel: exit_to_user_mode_prepare+0x1a6/0x1b0 Sep 07 11:55:32 debian9 kernel: syscall_exit_to_user_mode+0x16/0x40 Sep 07 11:55:32 debian9 kernel: do_syscall_64+0x48/0x90 Sep 07 11:55:32 debian9 kernel: entry_SYSCALL_64_after_hwframe+0x63/0xcd Sep 07 11:55:32 debian9 kernel: RIP: 0033:0x7fcde59a57a7 Sep 07 11:55:32 debian9 kernel: RSP: 002b:00007ffe914217c8 EFLAGS: 00000246 ORIG_RAX: 00000000000000a6 Sep 07 11:55:32 debian9 kernel: RAX: 0000000000000000 RBX: 00007fcde5ae8264 RCX: 00007fcde59a57a7 Sep 07 11:55:32 debian9 kernel: RDX: 0000000000000000 RSI: 0000000000000000 RDI: 000055b57556cdd0 Sep 07 11:55:32 debian9 kernel: RBP: 000055b57556cba0 R08: 0000000000000000 R09: 00007ffe91420570 Sep 07 11:55:32 debian9 kernel: R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 Sep 07 11:55:32 debian9 kernel: R13: 000055b57556cdd0 R14: 000055b57556ccb8 R15: 0000000000000000 Sep 07 11:55:32 debian9 kernel: </TASK> What happens is the following: 1) The cleaner kthread tries to start a transaction to delete an unused block group, but the metadata reservation can not be satisfied right away, so a reservation ticket is created and it starts the async metadata reclaim task (fs_info->async_reclaim_work); 2) Writeback for all the filler inodes with an i_size of 2K starts (generic/562 creates a lot of 2K files with the goal of filling metadata space). We try to create an inline extent for them, but we fail when trying to insert the inline extent with -ENOSPC (at cow_file_range_inline()) - since this is not critical, we fallback to non-inline mode (back to cow_file_range()), reserve extents ---truncated--- | N/A | More Details |
| CVE-2024-23527 | An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an unauthenticated remote attacker to read sensitive information in memory. | N/A | More Details |
| CVE-2022-48649 | In the Linux kernel, the following vulnerability has been resolved: mm/slab_common: fix possible double free of kmem_cache When doing slub_debug test, kfence's 'test_memcache_typesafe_by_rcu' kunit test case cause a use-after-free error: BUG: KASAN: use-after-free in kobject_del+0x14/0x30 Read of size 8 at addr ffff888007679090 by task kunit_try_catch/261 CPU: 1 PID: 261 Comm: kunit_try_catch Tainted: G B N 6.0.0-rc5-next-20220916 #17 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x34/0x48 print_address_description.constprop.0+0x87/0x2a5 print_report+0x103/0x1ed kasan_report+0xb7/0x140 kobject_del+0x14/0x30 kmem_cache_destroy+0x130/0x170 test_exit+0x1a/0x30 kunit_try_run_case+0xad/0xc0 kunit_generic_run_threadfn_adapter+0x26/0x50 kthread+0x17b/0x1b0 </TASK> The cause is inside kmem_cache_destroy(): kmem_cache_destroy acquire lock/mutex shutdown_cache schedule_work(kmem_cache_release) (if RCU flag set) release lock/mutex kmem_cache_release (if RCU flag not set) In some certain timing, the scheduled work could be run before the next RCU flag checking, which can then get a wrong value and lead to double kmem_cache_release(). Fix it by caching the RCU flag inside protected area, just like 'refcnt' | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2022-48652 | In the Linux kernel, the following vulnerability has been resolved: ice: Fix crash by keep old cfg when update TCs more than queues There are problems if allocated queues less than Traffic Classes. Commit a632b2a4c920 ("ice: ethtool: Prohibit improper channel config for DCB") already disallow setting less queues than TCs. Another case is if we first set less queues, and later update more TCs config due to LLDP, ice_vsi_cfg_tc() will failed but left dirty num_txq/rxq and tc_cfg in vsi, that will cause invalid pointer access. [ 95.968089] ice 0000:3b:00.1: More TCs defined than queues/rings allocated. [ 95.968092] ice 0000:3b:00.1: Trying to use more Rx queues (8), than were allocated (1)! [ 95.968093] ice 0000:3b:00.1: Failed to config TC for VSI index: 0 [ 95.969621] general protection fault: 0000 [#1] SMP NOPTI [ 95.969705] CPU: 1 PID: 58405 Comm: lldpad Kdump: loaded Tainted: G U W O --------- -t - 4.18.0 #1 [ 95.969867] Hardware name: O.E.M/BC11SPSCB10, BIOS 8.23 12/30/2021 [ 95.969992] RIP: 0010:devm_kmalloc+0xa/0x60 [ 95.970052] Code: 5c ff ff ff 31 c0 5b 5d 41 5c c3 b8 f4 ff ff ff eb f4 0f 1f 40 00 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 89 d1 <8b> 97 60 02 00 00 48 8d 7e 18 48 39 f7 72 3f 55 89 ce 53 48 8b 4c [ 95.970344] RSP: 0018:ffffc9003f553888 EFLAGS: 00010206 [ 95.970425] RAX: dead000000000200 RBX: ffffea003c425b00 RCX: 00000000006080c0 [ 95.970536] RDX: 00000000006080c0 RSI: 0000000000000200 RDI: dead000000000200 [ 95.970648] RBP: dead000000000200 R08: 00000000000463c0 R09: ffff888ffa900000 [ 95.970760] R10: 0000000000000000 R11: 0000000000000002 R12: ffff888ff6b40100 [ 95.970870] R13: ffff888ff6a55018 R14: 0000000000000000 R15: ffff888ff6a55460 [ 95.970981] FS: 00007f51b7d24700(0000) GS:ffff88903ee80000(0000) knlGS:0000000000000000 [ 95.971108] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [ 95.971197] CR2: 00007fac5410d710 CR3: 0000000f2c1de002 CR4: 00000000007606e0 [ 95.971309] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [ 95.971419] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [ 95.971530] PKRU: 55555554 [ 95.971573] Call Trace: [ 95.971622] ice_setup_rx_ring+0x39/0x110 [ice] [ 95.971695] ice_vsi_setup_rx_rings+0x54/0x90 [ice] [ 95.971774] ice_vsi_open+0x25/0x120 [ice] [ 95.971843] ice_open_internal+0xb8/0x1f0 [ice] [ 95.971919] ice_ena_vsi+0x4f/0xd0 [ice] [ 95.971987] ice_dcb_ena_dis_vsi.constprop.5+0x29/0x90 [ice] [ 95.972082] ice_pf_dcb_cfg+0x29a/0x380 [ice] [ 95.972154] ice_dcbnl_setets+0x174/0x1b0 [ice] [ 95.972220] dcbnl_ieee_set+0x89/0x230 [ 95.972279] ? dcbnl_ieee_del+0x150/0x150 [ 95.972341] dcb_doit+0x124/0x1b0 [ 95.972392] rtnetlink_rcv_msg+0x243/0x2f0 [ 95.972457] ? dcb_doit+0x14d/0x1b0 [ 95.972510] ? __kmalloc_node_track_caller+0x1d3/0x280 [ 95.972591] ? rtnl_calcit.isra.31+0x100/0x100 [ 95.972661] netlink_rcv_skb+0xcf/0xf0 [ 95.972720] netlink_unicast+0x16d/0x220 [ 95.972781] netlink_sendmsg+0x2ba/0x3a0 [ 95.975891] sock_sendmsg+0x4c/0x50 [ 95.979032] ___sys_sendmsg+0x2e4/0x300 [ 95.982147] ? kmem_cache_alloc+0x13e/0x190 [ 95.985242] ? __wake_up_common_lock+0x79/0x90 [ 95.988338] ? __check_object_size+0xac/0x1b0 [ 95.991440] ? _copy_to_user+0x22/0x30 [ 95.994539] ? move_addr_to_user+0xbb/0xd0 [ 95.997619] ? __sys_sendmsg+0x53/0x80 [ 96.000664] __sys_sendmsg+0x53/0x80 [ 96.003747] do_syscall_64+0x5b/0x1d0 [ 96.006862] entry_SYSCALL_64_after_hwframe+0x65/0xca Only update num_txq/rxq when passed check, and restore tc_cfg if setup queue map failed. | N/A | More Details |
| CVE-2024-22632 | Setor Informatica Sistema Inteligente para Laboratorios (S.I.L.) 388 was discovered to contain a remote code execution (RCE) vulnerability via the hmsg parameter. This vulnerability is triggered via a crafted POST request. | N/A | More Details |
| CVE-2022-48653 | In the Linux kernel, the following vulnerability has been resolved: ice: Don't double unplug aux on peer initiated reset In the IDC callback that is accessed when the aux drivers request a reset, the function to unplug the aux devices is called. This function is also called in the ice_prepare_for_reset function. This double call is causing a "scheduling while atomic" BUG. [ 662.676430] ice 0000:4c:00.0 rocep76s0: cqp opcode = 0x1 maj_err_code = 0xffff min_err_code = 0x8003 [ 662.676609] ice 0000:4c:00.0 rocep76s0: [Modify QP Cmd Error][op_code=8] status=-29 waiting=1 completion_err=1 maj=0xffff min=0x8003 [ 662.815006] ice 0000:4c:00.0 rocep76s0: ICE OICR event notification: oicr = 0x10000003 [ 662.815014] ice 0000:4c:00.0 rocep76s0: critical PE Error, GLPE_CRITERR=0x00011424 [ 662.815017] ice 0000:4c:00.0 rocep76s0: Requesting a reset [ 662.815475] BUG: scheduling while atomic: swapper/37/0/0x00010002 [ 662.815475] BUG: scheduling while atomic: swapper/37/0/0x00010002 [ 662.815477] Modules linked in: rpcsec_gss_krb5 auth_rpcgss nfsv4 dns_resolver nfs lockd grace fscache netfs rfkill 8021q garp mrp stp llc vfat fat rpcrdma intel_rapl_msr intel_rapl_common sunrpc i10nm_edac rdma_ucm nfit ib_srpt libnvdimm ib_isert iscsi_target_mod x86_pkg_temp_thermal intel_powerclamp coretemp target_core_mod snd_hda_intel ib_iser snd_intel_dspcfg libiscsi snd_intel_sdw_acpi scsi_transport_iscsi kvm_intel iTCO_wdt rdma_cm snd_hda_codec kvm iw_cm ipmi_ssif iTCO_vendor_support snd_hda_core irqbypass crct10dif_pclmul crc32_pclmul ghash_clmulni_intel snd_hwdep snd_seq snd_seq_device rapl snd_pcm snd_timer isst_if_mbox_pci pcspkr isst_if_mmio irdma intel_uncore idxd acpi_ipmi joydev isst_if_common snd mei_me idxd_bus ipmi_si soundcore i2c_i801 mei ipmi_devintf i2c_smbus i2c_ismt ipmi_msghandler acpi_power_meter acpi_pad rv(OE) ib_uverbs ib_cm ib_core xfs libcrc32c ast i2c_algo_bit drm_vram_helper drm_kms_helper syscopyarea sysfillrect sysimgblt fb_sys_fops drm_ttm_helpe r ttm [ 662.815546] nvme nvme_core ice drm crc32c_intel i40e t10_pi wmi pinctrl_emmitsburg dm_mirror dm_region_hash dm_log dm_mod fuse [ 662.815557] Preemption disabled at: [ 662.815558] [<0000000000000000>] 0x0 [ 662.815563] CPU: 37 PID: 0 Comm: swapper/37 Kdump: loaded Tainted: G S OE 5.17.1 #2 [ 662.815566] Hardware name: Intel Corporation D50DNP/D50DNP, BIOS SE5C6301.86B.6624.D18.2111021741 11/02/2021 [ 662.815568] Call Trace: [ 662.815572] <IRQ> [ 662.815574] dump_stack_lvl+0x33/0x42 [ 662.815581] __schedule_bug.cold.147+0x7d/0x8a [ 662.815588] __schedule+0x798/0x990 [ 662.815595] schedule+0x44/0xc0 [ 662.815597] schedule_preempt_disabled+0x14/0x20 [ 662.815600] __mutex_lock.isra.11+0x46c/0x490 [ 662.815603] ? __ibdev_printk+0x76/0xc0 [ib_core] [ 662.815633] device_del+0x37/0x3d0 [ 662.815639] ice_unplug_aux_dev+0x1a/0x40 [ice] [ 662.815674] ice_schedule_reset+0x3c/0xd0 [ice] [ 662.815693] irdma_iidc_event_handler.cold.7+0xb6/0xd3 [irdma] [ 662.815712] ? bitmap_find_next_zero_area_off+0x45/0xa0 [ 662.815719] ice_send_event_to_aux+0x54/0x70 [ice] [ 662.815741] ice_misc_intr+0x21d/0x2d0 [ice] [ 662.815756] __handle_irq_event_percpu+0x4c/0x180 [ 662.815762] handle_irq_event_percpu+0xf/0x40 [ 662.815764] handle_irq_event+0x34/0x60 [ 662.815766] handle_edge_irq+0x9a/0x1c0 [ 662.815770] __common_interrupt+0x62/0x100 [ 662.815774] common_interrupt+0xb4/0xd0 [ 662.815779] </IRQ> [ 662.815780] <TASK> [ 662.815780] asm_common_interrupt+0x1e/0x40 [ 662.815785] RIP: 0010:cpuidle_enter_state+0xd6/0x380 [ 662.815789] Code: 49 89 c4 0f 1f 44 00 00 31 ff e8 65 d7 95 ff 45 84 ff 74 12 9c 58 f6 c4 02 0f 85 64 02 00 00 31 ff e8 ae c5 9c ff fb 45 85 f6 <0f> 88 12 01 00 00 49 63 d6 4c 2b 24 24 48 8d 04 52 48 8d 04 82 49 [ 662.815791] RSP: 0018:ff2c2c4f18edbe80 EFLAGS: 00000202 [ 662.815793] RAX: ff280805df140000 RBX: 0000000000000002 RCX: 000000000000001f [ 662.815795] RDX: 0000009a52da2d08 R ---truncated--- | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48663 | In the Linux kernel, the following vulnerability has been resolved: gpio: mockup: fix NULL pointer dereference when removing debugfs We now remove the device's debugfs entries when unbinding the driver. This now causes a NULL-pointer dereference on module exit because the platform devices are unregistered *after* the global debugfs directory has been recursively removed. Fix it by unregistering the devices first. | N/A | More Details |
| CVE-2022-48665 | In the Linux kernel, the following vulnerability has been resolved: exfat: fix overflow for large capacity partition Using int type for sector index, there will be overflow in a large capacity partition. For example, if storage with sector size of 512 bytes and partition capacity is larger than 2TB, there will be overflow. | N/A | More Details |
| CVE-2024-26928 | In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in cifs_debug_files_proc_show() Skip sessions that are being teared down (status == SES_EXITING) to avoid UAF. | N/A | More Details |
| CVE-2024-3075 | The MM-email2image WordPress plugin through 0.2.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | N/A | More Details |
| CVE-2022-48667 | In the Linux kernel, the following vulnerability has been resolved: smb3: fix temporary data corruption in insert range insert range doesn't discard the affected cached region so can risk temporarily corrupting file data. Also includes some minor cleanup (avoiding rereading inode size repeatedly unnecessarily) to make it clearer. | N/A | More Details |
| CVE-2024-33339 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Details |
| CVE-2022-48668 | In the Linux kernel, the following vulnerability has been resolved: smb3: fix temporary data corruption in collapse range collapse range doesn't discard the affected cached region so can risk temporarily corrupting the file data. This fixes xfstest generic/031 I also decided to merge a minor cleanup to this into the same patch (avoiding rereading inode size repeatedly unnecessarily) to make it clearer. | N/A | More Details |
| CVE-2024-33401 | Cross Site Scripting vulnerability in DedeCMS v.5.7.113 allows a remote attacker to run arbitrary code via the mnum parameter. | N/A | More Details |
| CVE-2024-33331 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-33891. Reason: This candidate is a reservation duplicate of CVE-2024-33891. Notes: All CVE users should reference CVE-2024-33891 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage. | N/A | More Details |
| CVE-2022-48648 | In the Linux kernel, the following vulnerability has been resolved: sfc: fix null pointer dereference in efx_hard_start_xmit Trying to get the channel from the tx_queue variable here is wrong because we can only be here if tx_queue is NULL, so we shouldn't dereference it. As the above comment in the code says, this is very unlikely to happen, but it's wrong anyway so let's fix it. I hit this issue because of a different bug that caused tx_queue to be NULL. If that happens, this is the error message that we get here: BUG: unable to handle kernel NULL pointer dereference at 0000000000000020 [...] RIP: 0010:efx_hard_start_xmit+0x153/0x170 [sfc] | N/A | More Details |
| CVE-2024-26923 | In the Linux kernel, the following vulnerability has been resolved: af_unix: Fix garbage collector racing against connect() Garbage collector does not take into account the risk of embryo getting enqueued during the garbage collection. If such embryo has a peer that carries SCM_RIGHTS, two consecutive passes of scan_children() may see a different set of children. Leading to an incorrectly elevated inflight count, and then a dangling pointer within the gc_inflight_list. sockets are AF_UNIX/SOCK_STREAM S is an unconnected socket L is a listening in-flight socket bound to addr, not in fdtable V's fd will be passed via sendmsg(), gets inflight count bumped connect(S, addr) sendmsg(S, [V]); close(V) __unix_gc() ---------- ---------- ---------- NS = unix_create1() skb1 = sock_wmalloc(NS) L = unix_find_other(addr) unix_state_lock(L) unix_peer(S) = NS // V count=1 inflight=0 NS = unix_peer(S) skb2 = sock_alloc() skb_queue_tail(NS, skb2[V]) // V became in-flight // V count=2 inflight=1 close(V) // V count=1 inflight=1 // GC candidate condition met for u in gc_inflight_list: if (total_refs == inflight_refs) add u to gc_candidates // gc_candidates={L, V} for u in gc_candidates: scan_children(u, dec_inflight) // embryo (skb1) was not // reachable from L yet, so V's // inflight remains unchanged __skb_queue_tail(L, skb1) unix_state_unlock(L) for u in gc_candidates: if (u.inflight) scan_children(u, inc_inflight_move_tail) // V count=1 inflight=2 (!) If there is a GC-candidate listening socket, lock/unlock its state. This makes GC wait until the end of any ongoing connect() to that socket. After flipping the lock, a possibly SCM-laden embryo is already enqueued. And if there is another embryo coming, it can not possibly carry SCM_RIGHTS. At this point, unix_inflight() can not happen because unix_gc_lock is already taken. Inflight graph remains unaffected. | N/A | More Details |
| CVE-2024-33247 | Sourcecodester Employee Task Management System v1.0 is vulnerable to SQL Injection via admin-manage-user.php. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48647 | In the Linux kernel, the following vulnerability has been resolved: sfc: fix TX channel offset when using legacy interrupts In legacy interrupt mode the tx_channel_offset was hardcoded to 1, but that's not correct if efx_sepparate_tx_channels is false. In that case, the offset is 0 because the tx queues are in the single existing channel at index 0, together with the rx queue. Without this fix, as soon as you try to send any traffic, it tries to get the tx queues from an uninitialized channel getting these errors: WARNING: CPU: 1 PID: 0 at drivers/net/ethernet/sfc/tx.c:540 efx_hard_start_xmit+0x12e/0x170 [sfc] [...] RIP: 0010:efx_hard_start_xmit+0x12e/0x170 [sfc] [...] Call Trace: <IRQ> dev_hard_start_xmit+0xd7/0x230 sch_direct_xmit+0x9f/0x360 __dev_queue_xmit+0x890/0xa40 [...] BUG: unable to handle kernel NULL pointer dereference at 0000000000000020 [...] RIP: 0010:efx_hard_start_xmit+0x153/0x170 [sfc] [...] Call Trace: <IRQ> dev_hard_start_xmit+0xd7/0x230 sch_direct_xmit+0x9f/0x360 __dev_queue_xmit+0x890/0xa40 [...] | N/A | More Details |
| CVE-2024-26925 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: release mutex after nft_gc_seq_end from abort path The commit mutex should not be released during the critical section between nft_gc_seq_begin() and nft_gc_seq_end(), otherwise, async GC worker could collect expired objects and get the released commit lock within the same GC sequence. nf_tables_module_autoload() temporarily releases the mutex to load module dependencies, then it goes back to replay the transaction again. Move it at the end of the abort phase after nft_gc_seq_end() is called. | N/A | More Details |
| CVE-2022-48645 | In the Linux kernel, the following vulnerability has been resolved: net: enetc: deny offload of tc-based TSN features on VF interfaces TSN features on the ENETC (taprio, cbs, gate, police) are configured through a mix of command BD ring messages and port registers: enetc_port_rd(), enetc_port_wr(). Port registers are a region of the ENETC memory map which are only accessible from the PCIe Physical Function. They are not accessible from the Virtual Functions. Moreover, attempting to access these registers crashes the kernel: $ echo 1 > /sys/bus/pci/devices/0000\:00\:00.0/sriov_numvfs pci 0000:00:01.0: [1957:ef00] type 00 class 0x020001 fsl_enetc_vf 0000:00:01.0: Adding to iommu group 15 fsl_enetc_vf 0000:00:01.0: enabling device (0000 -> 0002) fsl_enetc_vf 0000:00:01.0 eno0vf0: renamed from eth0 $ tc qdisc replace dev eno0vf0 root taprio num_tc 8 map 0 1 2 3 4 5 6 7 \ queues 1@0 1@1 1@2 1@3 1@4 1@5 1@6 1@7 base-time 0 \ sched-entry S 0x7f 900000 sched-entry S 0x80 100000 flags 0x2 Unable to handle kernel paging request at virtual address ffff800009551a08 Internal error: Oops: 96000007 [#1] PREEMPT SMP pc : enetc_setup_tc_taprio+0x170/0x47c lr : enetc_setup_tc_taprio+0x16c/0x47c Call trace: enetc_setup_tc_taprio+0x170/0x47c enetc_setup_tc+0x38/0x2dc taprio_change+0x43c/0x970 taprio_init+0x188/0x1e0 qdisc_create+0x114/0x470 tc_modify_qdisc+0x1fc/0x6c0 rtnetlink_rcv_msg+0x12c/0x390 Split enetc_setup_tc() into separate functions for the PF and for the VF drivers. Also remove enetc_qos.o from being included into enetc-vf.ko, since it serves absolutely no purpose there. | N/A | More Details |
| CVE-2024-26926 | In the Linux kernel, the following vulnerability has been resolved: binder: check offset alignment in binder_get_object() Commit 6d98eb95b450 ("binder: avoid potential data leakage when copying txn") introduced changes to how binder objects are copied. In doing so, it unintentionally removed an offset alignment check done through calls to binder_alloc_copy_from_buffer() -> check_buffer(). These calls were replaced in binder_get_object() with copy_from_user(), so now an explicit offset alignment check is needed here. This avoids later complications when unwinding the objects gets harder. It is worth noting this check existed prior to commit 7a67a39320df ("binder: add function to copy binder object from buffer"), likely removed due to redundancy at the time. | N/A | More Details |
| CVE-2022-48644 | In the Linux kernel, the following vulnerability has been resolved: net/sched: taprio: avoid disabling offload when it was never enabled In an incredibly strange API design decision, qdisc->destroy() gets called even if qdisc->init() never succeeded, not exclusively since commit 87b60cfacf9f ("net_sched: fix error recovery at qdisc creation"), but apparently also earlier (in the case of qdisc_create_dflt()). The taprio qdisc does not fully acknowledge this when it attempts full offload, because it starts off with q->flags = TAPRIO_FLAGS_INVALID in taprio_init(), then it replaces q->flags with TCA_TAPRIO_ATTR_FLAGS parsed from netlink (in taprio_change(), tail called from taprio_init()). But in taprio_destroy(), we call taprio_disable_offload(), and this determines what to do based on FULL_OFFLOAD_IS_ENABLED(q->flags). But looking at the implementation of FULL_OFFLOAD_IS_ENABLED() (a bitwise check of bit 1 in q->flags), it is invalid to call this macro on q->flags when it contains TAPRIO_FLAGS_INVALID, because that is set to U32_MAX, and therefore FULL_OFFLOAD_IS_ENABLED() will return true on an invalid set of flags. As a result, it is possible to crash the kernel if user space forces an error between setting q->flags = TAPRIO_FLAGS_INVALID, and the calling of taprio_enable_offload(). This is because drivers do not expect the offload to be disabled when it was never enabled. The error that we force here is to attach taprio as a non-root qdisc, but instead as child of an mqprio root qdisc: $ tc qdisc add dev swp0 root handle 1: \ mqprio num_tc 8 map 0 1 2 3 4 5 6 7 \ queues 1@0 1@1 1@2 1@3 1@4 1@5 1@6 1@7 hw 0 $ tc qdisc replace dev swp0 parent 1:1 \ taprio num_tc 8 map 0 1 2 3 4 5 6 7 \ queues 1@0 1@1 1@2 1@3 1@4 1@5 1@6 1@7 base-time 0 \ sched-entry S 0x7f 990000 sched-entry S 0x80 100000 \ flags 0x0 clockid CLOCK_TAI Unable to handle kernel paging request at virtual address ffffffffffffffff8 [ffffffffffffffff8] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 96000004 [#1] PREEMPT SMP Call trace: taprio_dump+0x27c/0x310 vsc9959_port_setup_tc+0x1f4/0x460 felix_port_setup_tc+0x24/0x3c dsa_slave_setup_tc+0x54/0x27c taprio_disable_offload.isra.0+0x58/0xe0 taprio_destroy+0x80/0x104 qdisc_create+0x240/0x470 tc_modify_qdisc+0x1fc/0x6b0 rtnetlink_rcv_msg+0x12c/0x390 netlink_rcv_skb+0x5c/0x130 rtnetlink_rcv+0x1c/0x2c Fix this by keeping track of the operations we made, and undo the offload only if we actually did it. I've added "bool offloaded" inside a 4 byte hole between "int clockid" and "atomic64_t picos_per_byte". Now the first cache line looks like below: $ pahole -C taprio_sched net/sched/sch_taprio.o struct taprio_sched { struct Qdisc * * qdiscs; /* 0 8 */ struct Qdisc * root; /* 8 8 */ u32 flags; /* 16 4 */ enum tk_offsets tk_offset; /* 20 4 */ int clockid; /* 24 4 */ bool offloaded; /* 28 1 */ /* XXX 3 bytes hole, try to pack */ atomic64_t picos_per_byte; /* 32 0 */ /* XXX 8 bytes hole, try to pack */ spinlock_t current_entry_lock; /* 40 0 */ /* XXX 8 bytes hole, try to pack */ struct sched_entry * current_entry; /* 48 8 */ struct sched_gate_list * oper_sched; /* 56 8 */ /* --- cacheline 1 boundary (64 bytes) --- */ | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48643 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix nft_counters_enabled underflow at nf_tables_addchain() syzbot is reporting underflow of nft_counters_enabled counter at nf_tables_addchain() [1], for commit 43eb8949cfdffa76 ("netfilter: nf_tables: do not leave chain stats enabled on error") missed that nf_tables_chain_destroy() after nft_basechain_init() in the error path of nf_tables_addchain() decrements the counter because nft_basechain_init() makes nft_is_base_chain() return true by setting NFT_CHAIN_BASE flag. Increment the counter immediately after returning from nft_basechain_init(). | N/A | More Details |
| CVE-2022-48642 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix percpu memory leak at nf_tables_addchain() It seems to me that percpu memory for chain stats started leaking since commit 3bc158f8d0330f0a ("netfilter: nf_tables: map basechain priority to hardware priority") when nft_chain_offload_priority() returned an error. | N/A | More Details |
| CVE-2022-48641 | In the Linux kernel, the following vulnerability has been resolved: netfilter: ebtables: fix memory leak when blob is malformed The bug fix was incomplete, it "replaced" crash with a memory leak. The old code had an assignment to "ret" embedded into the conditional, restore this. | N/A | More Details |
| CVE-2022-48640 | In the Linux kernel, the following vulnerability has been resolved: bonding: fix NULL deref in bond_rr_gen_slave_id Fix a NULL dereference of the struct bonding.rr_tx_counter member because if a bond is initially created with an initial mode != zero (Round Robin) the memory required for the counter is never created and when the mode is changed there is never any attempt to verify the memory is allocated upon switching modes. This causes the following Oops on an aarch64 machine: [ 334.686773] Unable to handle kernel paging request at virtual address ffff2c91ac905000 [ 334.694703] Mem abort info: [ 334.697486] ESR = 0x0000000096000004 [ 334.701234] EC = 0x25: DABT (current EL), IL = 32 bits [ 334.706536] SET = 0, FnV = 0 [ 334.709579] EA = 0, S1PTW = 0 [ 334.712719] FSC = 0x04: level 0 translation fault [ 334.717586] Data abort info: [ 334.720454] ISV = 0, ISS = 0x00000004 [ 334.724288] CM = 0, WnR = 0 [ 334.727244] swapper pgtable: 4k pages, 48-bit VAs, pgdp=000008044d662000 [ 334.733944] [ffff2c91ac905000] pgd=0000000000000000, p4d=0000000000000000 [ 334.740734] Internal error: Oops: 96000004 [#1] SMP [ 334.745602] Modules linked in: bonding tls veth rfkill sunrpc arm_spe_pmu vfat fat acpi_ipmi ipmi_ssif ixgbe igb i40e mdio ipmi_devintf ipmi_msghandler arm_cmn arm_dsu_pmu cppc_cpufreq acpi_tad fuse zram crct10dif_ce ast ghash_ce sbsa_gwdt nvme drm_vram_helper drm_ttm_helper nvme_core ttm xgene_hwmon [ 334.772217] CPU: 7 PID: 2214 Comm: ping Not tainted 6.0.0-rc4-00133-g64ae13ed4784 #4 [ 334.779950] Hardware name: GIGABYTE R272-P31-00/MP32-AR1-00, BIOS F18v (SCP: 1.08.20211002) 12/01/2021 [ 334.789244] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [ 334.796196] pc : bond_rr_gen_slave_id+0x40/0x124 [bonding] [ 334.801691] lr : bond_xmit_roundrobin_slave_get+0x38/0xdc [bonding] [ 334.807962] sp : ffff8000221733e0 [ 334.811265] x29: ffff8000221733e0 x28: ffffdbac8572d198 x27: ffff80002217357c [ 334.818392] x26: 000000000000002a x25: ffffdbacb33ee000 x24: ffff07ff980fa000 [ 334.825519] x23: ffffdbacb2e398ba x22: ffff07ff98102000 x21: ffff07ff981029c0 [ 334.832646] x20: 0000000000000001 x19: ffff07ff981029c0 x18: 0000000000000014 [ 334.839773] x17: 0000000000000000 x16: ffffdbacb1004364 x15: 0000aaaabe2f5a62 [ 334.846899] x14: ffff07ff8e55d968 x13: ffff07ff8e55db30 x12: 0000000000000000 [ 334.854026] x11: ffffdbacb21532e8 x10: 0000000000000001 x9 : ffffdbac857178ec [ 334.861153] x8 : ffff07ff9f6e5a28 x7 : 0000000000000000 x6 : 000000007c2b3742 [ 334.868279] x5 : ffff2c91ac905000 x4 : ffff2c91ac905000 x3 : ffff07ff9f554400 [ 334.875406] x2 : ffff2c91ac905000 x1 : 0000000000000001 x0 : ffff07ff981029c0 [ 334.882532] Call trace: [ 334.884967] bond_rr_gen_slave_id+0x40/0x124 [bonding] [ 334.890109] bond_xmit_roundrobin_slave_get+0x38/0xdc [bonding] [ 334.896033] __bond_start_xmit+0x128/0x3a0 [bonding] [ 334.901001] bond_start_xmit+0x54/0xb0 [bonding] [ 334.905622] dev_hard_start_xmit+0xb4/0x220 [ 334.909798] __dev_queue_xmit+0x1a0/0x720 [ 334.913799] arp_xmit+0x3c/0xbc [ 334.916932] arp_send_dst+0x98/0xd0 [ 334.920410] arp_solicit+0xe8/0x230 [ 334.923888] neigh_probe+0x60/0xb0 [ 334.927279] __neigh_event_send+0x3b0/0x470 [ 334.931453] neigh_resolve_output+0x70/0x90 [ 334.935626] ip_finish_output2+0x158/0x514 [ 334.939714] __ip_finish_output+0xac/0x1a4 [ 334.943800] ip_finish_output+0x40/0xfc [ 334.947626] ip_output+0xf8/0x1a4 [ 334.950931] ip_send_skb+0x5c/0x100 [ 334.954410] ip_push_pending_frames+0x3c/0x60 [ 334.958758] raw_sendmsg+0x458/0x6d0 [ 334.962325] inet_sendmsg+0x50/0x80 [ 334.965805] sock_sendmsg+0x60/0x6c [ 334.969286] __sys_sendto+0xc8/0x134 [ 334.972853] __arm64_sys_sendto+0x34/0x4c ---truncated--- | N/A | More Details |
| CVE-2024-29205 | An Improper Check for Unusual or Exceptional Conditions vulnerability in the web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a remote unauthenticated attacker to send specially crafted requests in-order-to cause service disruptions. | N/A | More Details |
| CVE-2022-48639 | In the Linux kernel, the following vulnerability has been resolved: net: sched: fix possible refcount leak in tc_new_tfilter() tfilter_put need to be called to put the refount got by tp->ops->get to avoid possible refcount leak when chain->tmplt_ops != NULL and chain->tmplt_ops != tp->ops. | N/A | More Details |
| CVE-2022-48637 | In the Linux kernel, the following vulnerability has been resolved: bnxt: prevent skb UAF after handing over to PTP worker When reading the timestamp is required bnxt_tx_int() hands over the ownership of the completed skb to the PTP worker. The skb should not be used afterwards, as the worker may run before the rest of our code and free the skb, leading to a use-after-free. Since dev_kfree_skb_any() accepts NULL make the loss of ownership more obvious and set skb to NULL. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48633 | In the Linux kernel, the following vulnerability has been resolved: drm/gma500: Fix WARN_ON(lock->magic != lock) error psb_gem_unpin() calls dma_resv_lock() but the underlying ww_mutex gets destroyed by drm_gem_object_release() move the drm_gem_object_release() call in psb_gem_free_object() to after the unpin to fix the below warning: [ 79.693962] ------------[ cut here ]------------ [ 79.693992] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [ 79.694015] WARNING: CPU: 0 PID: 240 at kernel/locking/mutex.c:582 __ww_mutex_lock.constprop.0+0x569/0xfb0 [ 79.694052] Modules linked in: rfcomm snd_seq_dummy snd_hrtimer qrtr bnep ath9k ath9k_common ath9k_hw snd_hda_codec_realtek snd_hda_codec_generic ledtrig_audio snd_hda_codec_hdmi snd_hda_intel ath3k snd_intel_dspcfg mac80211 snd_intel_sdw_acpi btusb snd_hda_codec btrtl btbcm btintel btmtk bluetooth at24 snd_hda_core snd_hwdep uvcvideo snd_seq libarc4 videobuf2_vmalloc ath videobuf2_memops videobuf2_v4l2 videobuf2_common snd_seq_device videodev acer_wmi intel_powerclamp coretemp mc snd_pcm joydev sparse_keymap ecdh_generic pcspkr wmi_bmof cfg80211 i2c_i801 i2c_smbus snd_timer snd r8169 rfkill lpc_ich soundcore acpi_cpufreq zram rtsx_pci_sdmmc mmc_core serio_raw rtsx_pci gma500_gfx(E) video wmi ip6_tables ip_tables i2c_dev fuse [ 79.694436] CPU: 0 PID: 240 Comm: plymouthd Tainted: G W E 6.0.0-rc3+ #490 [ 79.694457] Hardware name: Packard Bell dot s/SJE01_CT, BIOS V1.10 07/23/2013 [ 79.694469] RIP: 0010:__ww_mutex_lock.constprop.0+0x569/0xfb0 [ 79.694496] Code: ff 85 c0 0f 84 15 fb ff ff 8b 05 ca 3c 11 01 85 c0 0f 85 07 fb ff ff 48 c7 c6 30 cb 84 aa 48 c7 c7 a3 e1 82 aa e8 ac 29 f8 ff <0f> 0b e9 ed fa ff ff e8 5b 83 8a ff 85 c0 74 10 44 8b 0d 98 3c 11 [ 79.694513] RSP: 0018:ffffad1dc048bbe0 EFLAGS: 00010282 [ 79.694623] RAX: 0000000000000028 RBX: 0000000000000000 RCX: 0000000000000000 [ 79.694636] RDX: 0000000000000001 RSI: ffffffffaa8b0ffc RDI: 00000000ffffffff [ 79.694650] RBP: ffffad1dc048bc80 R08: 0000000000000000 R09: ffffad1dc048ba90 [ 79.694662] R10: 0000000000000003 R11: ffffffffaad62fe8 R12: ffff9ff302103138 [ 79.694675] R13: ffff9ff306ec8000 R14: ffff9ff307779078 R15: ffff9ff3014c0270 [ 79.694690] FS: 00007ff1cccf1740(0000) GS:ffff9ff3bc200000(0000) knlGS:0000000000000000 [ 79.694705] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [ 79.694719] CR2: 0000559ecbcb4420 CR3: 0000000013210000 CR4: 00000000000006f0 [ 79.694734] Call Trace: [ 79.694749] <TASK> [ 79.694761] ? __schedule+0x47f/0x1670 [ 79.694796] ? psb_gem_unpin+0x27/0x1a0 [gma500_gfx] [ 79.694830] ? lock_is_held_type+0xe3/0x140 [ 79.694864] ? ww_mutex_lock+0x38/0xa0 [ 79.694885] ? __cond_resched+0x1c/0x30 [ 79.694902] ww_mutex_lock+0x38/0xa0 [ 79.694925] psb_gem_unpin+0x27/0x1a0 [gma500_gfx] [ 79.694964] psb_gem_unpin+0x199/0x1a0 [gma500_gfx] [ 79.694996] drm_gem_object_release_handle+0x50/0x60 [ 79.695020] ? drm_gem_object_handle_put_unlocked+0xf0/0xf0 [ 79.695042] idr_for_each+0x4b/0xb0 [ 79.695066] ? _raw_spin_unlock_irqrestore+0x30/0x60 [ 79.695095] drm_gem_release+0x1c/0x30 [ 79.695118] drm_file_free.part.0+0x1ea/0x260 [ 79.695150] drm_release+0x6a/0x120 [ 79.695175] __fput+0x9f/0x260 [ 79.695203] task_work_run+0x59/0xa0 [ 79.695227] do_exit+0x387/0xbe0 [ 79.695250] ? seqcount_lockdep_reader_access.constprop.0+0x82/0x90 [ 79.695275] ? lockdep_hardirqs_on+0x7d/0x100 [ 79.695304] do_group_exit+0x33/0xb0 [ 79.695331] __x64_sys_exit_group+0x14/0x20 [ 79.695353] do_syscall_64+0x58/0x80 [ 79.695376] ? up_read+0x17/0x20 [ 79.695401] ? lock_is_held_type+0xe3/0x140 [ 79.695429] ? asm_exc_page_fault+0x22/0x30 [ 79.695450] ? lockdep_hardirqs_on+0x7d/0x100 [ 79.695473] entry_SYSCALL_64_after_hwframe+0x63/0xcd [ 79.695493] RIP: 0033:0x7ff1ccefe3f1 [ 79.695516] Code: Unable to access opcode bytes at RIP 0x7ff1ccefe3c7. [ 79.695607] RSP: 002b:00007ffed4413378 EFLAGS: ---truncated--- | N/A | More Details |
| CVE-2022-48631 | In the Linux kernel, the following vulnerability has been resolved: ext4: fix bug in extents parsing when eh_entries == 0 and eh_depth > 0 When walking through an inode extents, the ext4_ext_binsearch_idx() function assumes that the extent header has been previously validated. However, there are no checks that verify that the number of entries (eh->eh_entries) is non-zero when depth is > 0. And this will lead to problems because the EXT_FIRST_INDEX() and EXT_LAST_INDEX() will return garbage and result in this: [ 135.245946] ------------[ cut here ]------------ [ 135.247579] kernel BUG at fs/ext4/extents.c:2258! [ 135.249045] invalid opcode: 0000 [#1] PREEMPT SMP [ 135.250320] CPU: 2 PID: 238 Comm: tmp118 Not tainted 5.19.0-rc8+ #4 [ 135.252067] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.15.0-0-g2dd4b9b-rebuilt.opensuse.org 04/01/2014 [ 135.255065] RIP: 0010:ext4_ext_map_blocks+0xc20/0xcb0 [ 135.256475] Code: [ 135.261433] RSP: 0018:ffffc900005939f8 EFLAGS: 00010246 [ 135.262847] RAX: 0000000000000024 RBX: ffffc90000593b70 RCX: 0000000000000023 [ 135.264765] RDX: ffff8880038e5f10 RSI: 0000000000000003 RDI: ffff8880046e922c [ 135.266670] RBP: ffff8880046e9348 R08: 0000000000000001 R09: ffff888002ca580c [ 135.268576] R10: 0000000000002602 R11: 0000000000000000 R12: 0000000000000024 [ 135.270477] R13: 0000000000000000 R14: 0000000000000024 R15: 0000000000000000 [ 135.272394] FS: 00007fdabdc56740(0000) GS:ffff88807dd00000(0000) knlGS:0000000000000000 [ 135.274510] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [ 135.276075] CR2: 00007ffc26bd4f00 CR3: 0000000006261004 CR4: 00000000000170ea0 [ 135.277952] Call Trace: [ 135.278635] <TASK> [ 135.279247] ? preempt_count_add+0x6d/0xa0 [ 135.280358] ? percpu_counter_add_batch+0x55/0xb0 [ 135.281612] ? _raw_read_unlock+0x18/0x30 [ 135.282704] ext4_map_blocks+0x294/0x5a0 [ 135.283745] ? xa_load+0x6f/0xa0 [ 135.284562] ext4_mpage_readpages+0x3d6/0x770 [ 135.285646] read_pages+0x67/0x1d0 [ 135.286492] ? folio_add_lru+0x51/0x80 [ 135.287441] page_cache_ra_unbounded+0x124/0x170 [ 135.288510] filemap_get_pages+0x23d/0x5a0 [ 135.289457] ? path_openat+0xa72/0xdd0 [ 135.290332] filemap_read+0xbf/0x300 [ 135.291158] ? _raw_spin_lock_irqsave+0x17/0x40 [ 135.292192] new_sync_read+0x103/0x170 [ 135.293014] vfs_read+0x15d/0x180 [ 135.293745] ksys_read+0xa1/0xe0 [ 135.294461] do_syscall_64+0x3c/0x80 [ 135.295284] entry_SYSCALL_64_after_hwframe+0x46/0xb0 This patch simply adds an extra check in __ext4_ext_check(), verifying that eh_entries is not 0 when eh_depth is > 0. | N/A | More Details |
| CVE-2024-28613 | SQL Injection vulnerability in PHP Task Management System v.1.0 allows a remote attacker to escalate privileges and obtain sensitive information via the task_id parameter of the task-details.php, and edit-task.php component. | N/A | More Details |