SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 24 April 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-2024-28189 | Judge0 is an open-source online code execution system. The application uses the UNIX chown command on an untrusted file within the sandbox. An attacker can abuse this by creating a symbolic link (symlink) to a file outside the sandbox, allowing the attacker to run chown on arbitrary files outside of the sandbox. This vulnerability is not impactful on it's own, but it can be used to bypass the patch for CVE-2024-28185 and obtain a complete sandbox escape. This vulnerability is fixed in 1.13.1. | 10.0 | More Details |
| CVE-2024-28185 | Judge0 is an open-source online code execution system. The application does not account for symlinks placed inside the sandbox directory, which can be leveraged by an attacker to write to arbitrary files and gain code execution outside of the sandbox. When executing a submission, Judge0 writes a `run_script` to the sandbox directory. The security issue is that an attacker can create a symbolic link (symlink) at the path `run_script` before this code is executed, resulting in the `f.write` writing to an arbitrary file on the unsandboxed system. An attacker can leverage this vulnerability to overwrite scripts on the system and gain code execution outside of the sandbox. | 10.0 | More Details |
| CVE-2024-32599 | Improper Control of Generation of Code ('Code Injection') vulnerability in Deepak anand WP Dummy Content Generator.This issue affects WP Dummy Content Generator: from n/a through 3.2.1. | 10.0 | More Details |
| CVE-2024-32514 | Unrestricted Upload of File with Dangerous Type vulnerability in Poll Maker & Voting Plugin Team (InfoTheme) WP Poll Maker.This issue affects WP Poll Maker: from n/a through 3.4. | 9.9 | More Details |
| CVE-2023-49742 | Missing Authorization vulnerability in Support Genix.This issue affects Support Genix: from n/a through 1.2.3. | 9.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-27348 | RCE-Remote Command Execution vulnerability in Apache HugeGraph-Server.This issue affects Apache HugeGraph-Server: from 1.0.0 before 1.3.0 in Java8 & Java11 Users are recommended to upgrade to version 1.3.0 with Java11 & enable the Auth system, which fixes the issue. | 9.8 | More Details |
| CVE-2023-47435 | An issue in the verifyPassword function of hexo-theme-matery v2.0.0 allows attackers to bypass authentication and access password protected pages. | 9.8 | More Details |
| CVE-2024-31546 | Computer Laboratory Management System v1.0 is vulnerable to SQL Injection via the "id" parameter of /admin/damage/view_damage.php. | 9.8 | More Details |
| CVE-2024-32418 | An issue in flusity CMS v2.33 allows a remote attacker to execute arbitrary code via the add_addon.php component. | 9.8 | More Details |
| CVE-2024-29661 | A File Upload vulnerability in DedeCMS v5.7 allows a local attacker to execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2024-32238 | H3C ER8300G2-X is vulnerable to Incorrect Access Control. The password for the router's management system can be accessed via the management system page login interface. | 9.8 | More Details |
| CVE-2024-31750 | SQL injection vulnerability in f-logic datacube3 v.1.0 allows a remote attacker to obtain sensitive information via the req_id parameter. | 9.8 | More Details |
| CVE-2024-4040 | A server side template injection vulnerability in CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server. | 9.8 | More Details |
| CVE-2024-32039 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients using a version of FreeRDP prior to 3.5.0 or 2.11.6 are vulnerable to integer overflow and out-of-bounds write. Versions 3.5.0 and 2.11.6 patch the issue. As a workaround, do not use `/gfx` options (e.g. deactivate with `/bpp:32` or `/rfx` as it is on by default). | 9.8 | More Details |
| CVE-2024-32041 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients that use a version of FreeRDP prior to 3.5.0 or 2.11.6 are vulnerable to out-of-bounds read. Versions 3.5.0 and 2.11.6 patch the issue. As a workaround, deactivate `/gfx` (on by default, set `/bpp` or `/rfx` options instead. | 9.8 | More Details |
| CVE-2024-32458 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients that use a version of FreeRDP prior to 3.5.0 or 2.11.6 are vulnerable to out-of-bounds read. Versions 3.5.0 and 2.11.6 patch the issue. As a workaround, use `/gfx` or `/rfx` modes (on by default, require server side support). | 9.8 | More Details |
| CVE-2024-32459 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients and servers that use a version of FreeRDP prior to 3.5.0 or 2.11.6 are vulnerable to out-of-bounds read. Versions 3.5.0 and 2.11.6 patch the issue. No known workarounds are available. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-21511 | Versions of the package mysql2 before 3.9.7 are vulnerable to Arbitrary Code Injection due to improper sanitization of the timezone parameter in the readCodeFor function by calling a native MySQL Server date/time function. | 9.8 | More Details |
| CVE-2024-33215 | Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the mitInterface parameter in ip/goform/addressNat. | 9.8 | More Details |
| CVE-2024-32658 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients prior to version 3.5.1 are vulnerable to out-of-bounds read. Version 3.5.1 contains a patch for the issue. No known workarounds are available. | 9.8 | More Details |
| CVE-2024-32038 | Wazuh is a free and open source platform used for threat prevention, detection, and response. There is a buffer overflow hazard in wazuh-analysisd when handling Unicode characters from Windows Eventchannel messages. It impacts Wazuh Manager 3.8.0 and above. This vulnerability is fixed in Wazuh Manager 4.7.2. | 9.8 | More Details |
| CVE-2024-30938 | SQL Injection vulnerability in SEMCMS v.4.8 allows a remote attacker to obtain sensitive information via the ID parameter in the SEMCMS_User.php component. | 9.8 | More Details |
| CVE-2024-32659 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients prior to version 3.5.1 are vulnerable to out-of-bounds read if `((nWidth == 0) and (nHeight == 0))`. Version 3.5.1 contains a patch for the issue. No known workarounds are available. | 9.8 | More Details |
| CVE-2024-32161 | jizhiCMS 2.5 suffers from a File upload vulnerability. | 9.8 | More Details |
| CVE-2024-30922 | SQL Injection vulnerability in DerbyNet v9.0 allows a remote attacker to execute arbitrary code via the where Clause in Award Document Rendering. | 9.8 | More Details |
| CVE-2024-32301 | Tenda AC7V1.0 v15.03.06.44 firmware has a stack overflow vulnerability via the PPW parameter in the fromWizardHandle function. | 9.8 | More Details |
| CVE-2024-30564 | An issue inandrei-tatar nora-firebase-common between v.1.0.41 and v.1.12.2 allows a remote attacker to execute arbitrary code via a crafted script to the updateState parameter of the updateStateInternal method. | 9.8 | More Details |
| CVE-2024-32286 | Tenda W30E v1.0 V1.0.1.25(633) firmware has a stack overflow vulnerability located via the page parameter in the fromVirtualSer function. | 9.8 | More Details |
| CVE-2024-32318 | Tenda AC500 V2.0.1.9(1307) firmware has a stack overflow vulnerability via the vlan parameter in the formSetVlanInfo function. | 9.8 | More Details |
| CVE-2024-30980 | SQL Injection vulnerability in phpgurukul Cyber Cafe Management System Using PHP & MySQL 1.0 allows attackers to run arbitrary SQL commands via the Computer Location parameter in manage-computer.php page. | 9.8 | More Details |
| CVE-2024-3817 | HashiCorp's go-getter library is vulnerable to argument injection when executing Git to discover remote branches. This vulnerability does not affect the go-getter/v2 branch and package. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-30982 | SQL Injection vulnerability in phpgurukul Cyber Cafe Management System Using PHP & MySQL 1.0 allows attackers to run arbitrary SQL commands via the upid parameter in the /view-user-detail.php file. | 9.8 | More Details |
| CVE-2024-30923 | SQL Injection vulnerability in DerbyNet v9.0 and below allows a remote attacker to execute arbitrary code via the where Clause in Racer Document Rendering | 9.8 | More Details |
| CVE-2024-31581 | FFmpeg version n6.1 was discovered to contain an improper validation of array index vulnerability in libavcodec/cbs_h266_syntax_template.c. This vulnerability allows attackers to cause undefined behavior within the application. | 9.8 | More Details |
| CVE-2024-30990 | SQL Injection vulnerability in the "Invoices" page in phpgurukul Client Management System using PHP & MySQL 1.1 allows attacker to execute arbitrary SQL commands via "searchdata" parameter. | 9.8 | More Details |
| CVE-2024-30985 | SQL Injection vulnerability in "B/W Dates Reports" page in phpgurukul Client Management System using PHP & MySQL 1.1 allows attacker to execute arbitrary SQL commands via "todate" and "fromdate" parameters. | 9.8 | More Details |
| CVE-2024-32340 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the WEBSITE TITLE parameter under the Menu module. | 9.6 | More Details |
| CVE-2024-31545 | Computer Laboratory Management System v1.0 is vulnerable to SQL Injection via the "id" parameter of /admin/?page=user/manage_user&id=6. | 9.4 | More Details |
| CVE-2024-2796 | A server-side request forgery (SSRF) was discovered in the Akana API Platform in versions prior to and including 2022.1.3. Reported by Jakob Antonsson. | 9.3 | More Details |
| CVE-2024-27574 | SQL Injection vulnerability in Trainme Academy version Ichin v.1.3.2 allows a remote attacker to obtain sensitive information via the informacion, idcurso, and tit parameters. | 9.1 | More Details |
| CVE-2024-27349 | Authentication Bypass by Spoofing vulnerability in Apache HugeGraph-Server.This issue affects Apache HugeGraph-Server: from 1.0.0 before 1.3.0. Users are recommended to upgrade to version 1.3.0, which fixes the issue. | 9.1 | More Details |
| CVE-2024-31547 | Computer Laboratory Management System v1.0 is vulnerable to SQL Injection via the "id" parameter of /admin/item/view_item.php. | 9.1 | More Details |
| CVE-2024-32644 | Evmos is a scalable, high-throughput Proof-of-Stake EVM blockchain that is fully compatible and interoperable with Ethereum. Prior to 17.0.0, there is a way to mint arbitrary tokens due to the possibility to have two different states not in sync during the execution of a transaction. The exploit is based on the fact that to sync the Cosmos SDK state and the EVM one, we rely on the `stateDB.Commit()` method. When we call this method, we iterate though all the `dirtyStorage` and, **if and only if** it is different than the `originStorage`, we set the new state. Setting the new state means we update the Cosmos SDK KVStore. If a contract storage state that is the same before and after a transaction, but is changed during the transaction and can call an external contract after the change, it can be exploited to make the transaction similar to non-atomic. The vulnerability is **critical** since this could lead to drain of funds through creative SC interactions. The issue has been patched in versions >=V17.0.0. | 9.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-39367 | An OS command injection vulnerability exists in the web interface mac2name functionality of Peplink Smart Reader v1.2.0 (in QEMU). A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. | 9.1 | More Details |
| CVE-2024-29021 | Judge0 is an open-source online code execution system. The default configuration of Judge0 leaves the service vulnerable to a sandbox escape via Server Side Request Forgery (SSRF). This allows an attacker with sufficient access to the Judge0 API to obtain unsandboxed code execution as root on the target machine. This vulnerability is fixed in 1.13.1. | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3909 | A vulnerability classified as critical was found in Tenda AC500 2.0.1.9(1307). Affected by this vulnerability is the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput 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-261145 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-2024-3834 | Use after free in Downloads in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) | 8.8 | More Details |
| CVE-2024-32292 | Tenda W30E v1.0 V1.0.1.25(633) firmware contains a command injection vulnerablility in the formexeCommand function via the cmdinput parameter. | 8.8 | More Details |
| CVE-2024-32299 | Tenda FH1203 v2.0.1.6 firmware has a stack overflow vulnerability via the PPW parameter in the fromWizardHandle function. | 8.8 | More Details |
| CVE-2024-3905 | A vulnerability was found in Tenda AC500 2.0.1.9(1307). It has been classified as critical. This affects the function R7WebsSecurityHandler of the file /goform/execCommand. The manipulation of the argument password 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-261141 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-2024-31680 | File Upload vulnerability in Shibang Communications Co., Ltd. IP network intercom broadcasting system v.1.0 allows a local attacker to execute arbitrary code via the my_parser.php component. | 8.8 | More Details |
| CVE-2024-3832 | Object corruption in V8 in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) | 8.8 | More Details |
| CVE-2024-3833 | Object corruption in WebAssembly in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) | 8.8 | More Details |
| CVE-2024-3837 | Use after free in QUIC in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) | 8.8 | More Details |
| CVE-2024-3906 | A vulnerability was found in Tenda AC500 2.0.1.9(1307). It has been declared as critical. This vulnerability affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword 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-261142 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-2023-38298 | Various software builds for the following TCL devices (30Z, A3X, 20XE, 10L) leak the device IMEI to a system property that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in these instances they are leaked by a high-privilege process and can be obtained indirectly. The software build fingerprints for each confirmed vulnerable device are as follows: TCL 30Z (TCL/4188R/Jetta_ATT:12/SP1A.210812.016/LV8E:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU5P:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU61:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU66:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU68:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU6P:user/release-keys, and TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU6X:user/release-keys); TCL A3X (TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAAZ:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAB3:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAB7:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABA:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABM:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABP:user/release-keys, and TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABS:user/release-keys); TCL 20XE (TCL/5087Z_BO/Doha_TMO:11/RP1A.200720.011/PB7I-0:user/release-keys and TCL/5087Z_BO/Doha_TMO:11/RP1A.200720.011/PB83-0:user/release-keys); and TCL 10L (TCL/T770B/T1_LITE:10/QKQ1.200329.002/3CJ0:user/release-keys and TCL/T770B/T1_LITE:11/RKQ1.210107.001/8BIC:user/release-keys). This malicious app reads from the "gsm.device.imei0" system property to indirectly obtain the device IMEI. | 8.8 | More Details |
| CVE-2024-22186 | The application suffers from a privilege escalation vulnerability. An attacker logged in as guest can escalate his privileges by poisoning the cookie to become administrator. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32305 | Tenda A18 v15.03.05.05 firmware has a stack overflow vulnerability located via the PPW parameter in the fromWizardHandle function. | 8.8 | More Details |
| CVE-2024-3293 | The rtMedia for WordPress, BuddyPress and bbPress plugin for WordPress is vulnerable to blind SQL Injection via the rtmedia_gallery shortcode in all versions up to, and including, 4.6.18 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | 8.8 | More Details |
| CVE-2024-32407 | An issue in inducer relate before v.2024.1 allows a remote attacker to execute arbitrary code via a crafted payload to the Page Sandbox feature. | 8.8 | More Details |
| CVE-2024-32394 | An issue in ruijie.com/cn RG-RSR10-01G-T(WA)-S RSR_3.0(1)B9P2_RSR10-01G-TW-S_07150910 and RG-RSR10-01G-T(WA)-S RSR_3.0(1)B9P2_RSR10-01G-TW-S_07150910 allows a remote attacker to execute arbitrary code via a crafted HTTP request. | 8.8 | More Details |
| CVE-2024-32166 | Webid v1.2.1 suffers from an Insecure Direct Object Reference (IDOR) - Broken Access Control vulnerability, allowing attackers to buy now an auction that is suspended (horizontal privilege escalation). | 8.8 | More Details |
| CVE-2024-4020 | A vulnerability was found in Tenda FH1206 1.2.0.8(8155) and classified as critical. This issue affects the function fromAddressNat of the file /goform/addressNat. The manipulation of the argument entrys leads to 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-261671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-33212 | Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the funcpara1 parameter in ip/goform/setcfm. | 8.8 | More Details |
| CVE-2024-4066 | A vulnerability classified as critical has been found in Tenda AC8 16.03.34.09. Affected is the function fromAdvSetMacMtuWan of the file /goform/AdvSetMacMtuWan. The manipulation of the argument wanMTU/wanSpeed/cloneType/mac/serviceName/serverName 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-261792. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-3910 | A vulnerability, which was classified as critical, has been found in Tenda AC500 2.0.1.9(1307). Affected by this issue is the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page 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-261146 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-2024-4017 | Improper Privilege Management vulnerability in BeyondTrust U-Series Appliance on Windows, 64 bit (filesystem modules) allows DLL Side-Loading.This issue affects U-Series Appliance: from 3.4 before 4.0.3. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-50260 | Wazuh is a free and open source platform used for threat prevention, detection, and response. A wrong validation in the `host_deny` script allows to write any string in the `hosts.deny` file, which can end in an arbitrary command execution on the target system. This vulnerability is part of the active response feature, which can automatically triggers actions in response to alerts. By default, active responses are limited to a set of pre defined executables. This is enforced by only allowing executables stored under `/var/ossec/active-response/bin` to be run as an active response. However, the `/var/ossec/active-response/bin/host_deny` can be exploited. `host_deny` is used to add IP address to the `/etc/hosts.deny` file to block incoming connections on a service level by using TCP wrappers. Attacker can inject arbitrary command into the `/etc/hosts.deny` file and execute arbitrary command by using the spawn directive. The active response can be triggered by writing events either to the local `execd` queue on server or to the `ar` queue which forwards the events to agents. So, it can leads to LPE on server as root and RCE on agent as root. This vulnerability is fixed in 4.7.2. | 8.8 | More Details |
| CVE-2024-32258 | The network server of fceux 2.7.0 has a path traversal vulnerability, allowing attackers to overwrite any files on the server without authentication by fake ROM. | 8.8 | More Details |
| CVE-2024-3907 | A vulnerability was found in Tenda AC500 2.0.1.9(1307). It has been rated as critical. This issue affects the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 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-261143. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 8.8 | More Details |
| CVE-2024-31616 | An issue discovered in RG-RSR10-01G-T(W)-S and RG-RSR10-01G-T(WA)-S routers with firmware version RSR10-01G-T-S_RSR_3.0(1)B9P2, Release(07150910) allows attackers to execute arbitrary code via the common_quick_config.lua file. | 8.8 | More Details |
| CVE-2024-32281 | Tenda AC7V1.0 v15.03.06.44 firmware contains a command injection vulnerablility in formexeCommand function via the cmdinput parameter. | 8.8 | More Details |
| CVE-2024-4018 | Improper Privilege Management vulnerability in BeyondTrust U-Series Appliance on Windows, 64 bit (local appliance api modules) allows Privilege Escalation.This issue affects U-Series Appliance: from 3.4 before 4.0.3. | 8.8 | More Details |
| CVE-2023-49963 | DYMO LabelWriter Print Server through 2.366 contains a backdoor hard-coded password that could allow an attacker to take control. | 8.8 | More Details |
| CVE-2024-4064 | A vulnerability was found in Tenda AC8 16.03.34.09. It has been declared as critical. This vulnerability affects the function R7WebsSecurityHandler of the file /goform/execCommand. The manipulation of the argument password 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-261790 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-2024-4065 | A vulnerability was found in Tenda AC8 16.03.34.09. It has been rated as critical. This issue affects the function formSetRebootTimer of the file /goform/SetRebootTimer. The manipulation of the argument rebootTime 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-261791. 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-2023-49502 | Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_bwdif_filter_intra_c function in the libavfilter/bwdifdsp.c:125:5 component. | 8.8 | More Details |
| CVE-2023-38292 | Certain software builds for the TCL 20XE Android device contain a vulnerable, pre-installed app with a package name of com.tct.gcs.hiddenmenuproxy (versionCode='2', versionName='v11.0.1.0.0201.0') that allows local third-party apps to programmatically perform a factory reset due to inadequate access control. No permissions or special privileges are necessary to exploit the vulnerability in the com.tct.gcs.hiddenmenuproxy app. No user interaction is required beyond installing and running a third-party app. The software build fingerprints for each confirmed vulnerable build are as follows: TCL/5087Z_BO/Doha_TMO:11/RP1A.200720.011/PB7I-0:user/release-keys and TCL/5087Z_BO/Doha_TMO:11/RP1A.200720.011/PB83-0:user/release-keys. This malicious app sends a broadcast intent to the exported com.tct.gcs.hiddenmenuproxy/.rtn.FactoryResetReceiver receiver component, which initiates a programmatic factory reset. | 8.7 | More Details |
| CVE-2024-29959 | A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a prints Brocade Fabric OS switch encrypted passwords in the Brocade SANnav Standby node's support save. | 8.6 | More Details |
| CVE-2022-47151 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.7.1. | 8.6 | More Details |
| CVE-2024-32866 | Conform, a type-safe form validation library, allows the parsing of nested objects in the form of `object.property`. Due to an improper implementation of this feature in versions prior to 1.1.1, an attacker can exploit the feature to trigger prototype pollution by passing a crafted input to `parseWith...` functions. Applications that use conform for server-side validation of form data or URL parameters are affected by this vulnerability. Version 1.1.1 contains a patch for the issue. | 8.6 | More Details |
| CVE-2024-32562 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VIICTORY MEDIA LLC Z Y N I T H allows Stored XSS.This issue affects Z Y N I T H: from n/a through 7.4.9. | 8.6 | More Details |
| CVE-2024-32603 | Deserialization of Untrusted Data vulnerability in ThemeKraft WooBuddy.This issue affects WooBuddy: from n/a through 3.4.20. | 8.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-38297 | An issue was discovered in a third-party com.factory.mmigroup component, shipped on devices from multiple device manufacturers. Certain software builds for various Android devices contain a vulnerable pre-installed app with a package name of com.factory.mmigroup (versionCode='3', versionName='2.1') that allows local third-party apps to perform various actions, due to inadequate access control, in its context (system user), but the functionalities exposed depend on the specific device. The following capabilities are exposed to zero-permission, third-party apps on the following devices: arbitrary AT command execution via AT command injection (T-Mobile Revvl 6 Pro 5G, T-Mobile Revvl V+ 5G, and Boost Mobile Celero 5G); programmatic factory reset (Samsung Galaxy A03S, T-Mobile Revvl 6 Pro 5G, T-Mobile Revvl V+ 5G, Boost Mobile Celero, Realme C25Y, and Lenovo Tab M8 HD), leaking IMEI (Samsung Galaxy A03S, T-Mobile Revvl 6 Pro 5G, T-Mobile Revvl V+ 5G, Boost Mobile Celero, and Realme C25Y); leaking serial number (Samsung Galaxy A03s, T-Mobile Revvl 6 Pro 5G, T-Mobile Revvl V+ 5G, Boost Mobile Celero, Realme C25Y, and Lenovo Tab M8 HD); powering off the device (Realme C25Y, Samsung Galaxy A03S, and T-Mobile Revvl 6 Pro 5G); and programmatically enabling/disabling airplane mode (Samsung Galaxy A03S, T-Mobile Revvl 6 Pro 5G, T-Mobile Revvl V+ 5G, Boost Mobile Celero, and Realme C25Y); and enabling Wi-Fi, Bluetooth, and GPS (Samsung Galaxy A03S, T-Mobile Revvl 6 Pro 5G, T-Mobile Revvl V+ 5G, Boost Mobile Celero, and Realme C25Y). No permissions or special privileges are necessary to exploit the vulnerabilities in the com.factory.mmigroup app. No user interaction is required beyond installing and running a third-party app. The software build fingerprints for each confirmed vulnerable device are as follows: Boost Mobile Celero 5G (Celero5G/Jupiter/Jupiter:11/RP1A.200720.011/SW_S98119AA1_V067:user/release-keys, Celero5G/Jupiter/Jupiter:11/RP1A.200720.011/SW_S98119AA1_V064:user/release-keys, Celero5G/Jupiter/Jupiter:11/RP1A.200720.011/SW_S98119AA1_V061:user/release-keys, and Celero5G/Jupiter/Jupiter:11/RP1A.200720.011/SW_S98119AA1_V052:user/release-keys); Samsung Galaxy A03S (samsung/a03sutfn/a03su:13/TP1A.220624.014/S134DLUDU6CWB6:user/release-keys and samsung/a03sutfn/a03su:12/SP1A.210812.016/S134DLUDS5BWA1:user/release-keys); Lenovo Tab M8 HD (Lenovo/LenovoTB-8505F/8505F:10/QP1A.190711.020/S300637_220706_BMP:user/release-keys and Lenovo/LenovoTB-8505F/8505F:10/QP1A.190711.020/S300448_220114_BMP:user/release-keys); T-Mobile Revvl 6 Pro 5G (T-Mobile/Augusta/Augusta:12/SP1A.210812.016/SW_S98121AA1_V070:user/release-keys and T-Mobile/Augusta/Augusta:12/SP1A.210812.016/SW_S98121AA1_V066:user/release-keys); T-Mobile Revvl V+ 5G (T-Mobile/Sprout/Sprout:11/RP1A.200720.011/SW_S98115AA1_V077:user/release-keys and T-Mobile/Sprout/Sprout:11/RP1A.200720.011/SW_S98115AA1_V060:user/release-keys); and Realme C25Y (realme/RMX3269/RED8F6:11/RP1A.201005.001/1675861640000:user/release-keys, realme/RMX3269/RED8F6:11/RP1A.201005.001/1664031768000:user/release-keys, realme/RMX3269/RED8F6:11/RP1A.201005.001/1652814687000:user/release-keys, and realme/RMX3269/RED8F6:11/RP1A.201005.001/1635785712000:user/release-keys). This malicious app sends a broadcast Intent to com.factory.mmigroup/.MMIGroupReceiver. This causes the com.factory.mmigroup app to dynamically register for various action strings. The malicious app can then send these strings, allowing it to perform various behaviors that the com.factory.mmigroup app exposes. The actual behaviors exposed by the com.factory.mmigroup app depend on device model and chipset. The com.factory.mmigroup app executes as the "system" user, allowing it to interact with the baseband processor and perform various other sensitive actions. | 8.4 | More Details |
| CVE-2024-28073 | SolarWinds Serv-U was found to be susceptible to a Directory Traversal Remote Code Vulnerability. This vulnerability requires a highly privileged account to be exploited. | 8.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32462 | Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. in versions before 1.10.9, 1.12.9, 1.14.6, and 1.15.8, a malicious or compromised Flatpak app could execute arbitrary code outside its sandbox. Normally, the `--command` argument of `flatpak run` expects to be given a command to run in the specified Flatpak app, optionally along with some arguments. However it is possible to instead pass `bwrap` arguments to `--command=`, such as `--bind`. It's possible to pass an arbitrary `commandline` to the portal interface `org.freedesktop.portal.Background.RequestBackground` from within a Flatpak app. When this is converted into a `--command` and arguments, it achieves the same effect of passing arguments directly to `bwrap`, and thus can be used for a sandbox escape. The solution is to pass the `--` argument to `bwrap`, which makes it stop processing options. This has been supported since bubblewrap 0.3.0. All supported versions of Flatpak require at least that version of bubblewrap. xdg-desktop-portal version 1.18.4 will mitigate this vulnerability by only allowing Flatpak apps to create .desktop files for commands that do not start with --. The vulnerability is patched in 1.15.8, 1.10.9, 1.12.9, and 1.14.6. | 8.4 | More Details |
| CVE-2024-32600 | Deserialization of Untrusted Data vulnerability in Averta Master Slider.This issue affects Master Slider: from n/a through 3.9.5. | 8.3 | More Details |
| CVE-2023-45744 | A data integrity vulnerability exists in the web interface /cgi-bin/upload_config.cgi functionality of Peplink Smart Reader v1.2.0 (in QEMU). A specially crafted HTTP request can lead to configuration modification. An attacker can make an unauthenticated HTTP request to trigger this vulnerability. | 8.3 | More Details |
| CVE-2024-3323 | Cross Site Scripting in UI Request/Response Validation in TIBCO JasperReports Server 8.0.4 and 8.2.0 allows allows for the injection of malicious executable scripts into the code of a trusted application that may lead to stealing the user's active session cookie via sending malicious link, enticing the user to interact. | 8.3 | More Details |
| CVE-2024-22811 | An issue in Tormach xsTECH CNC Router, PathPilot Controller v2.9.6 allows attackers to cause a Denial of Service (DoS) by disrupting the communication between the PathPilot controller and the CNC router via overwriting the Hostmot2 configuration cookie in the device memory. | 8.2 | More Details |
| CVE-2024-29961 | A vulnerability affects Brocade SANnav before v2.3.1 and v2.3.0a. It allows a Brocade SANnav service to send ping commands in the background at regular intervals to gridgain.com to check if updates are available for the Component. This could make an unauthenticated, remote attacker aware of the behavior and launch a supply-chain attack against a Brocade SANnav appliance. | 8.2 | More Details |
| CVE-2024-32460 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based based clients using `/bpp:32` legacy `GDI` drawing path with a version of FreeRDP prior to 3.5.0 or 2.11.6 are vulnerable to out-of-bounds read. Versions 3.5.0 and 2.11.6 patch the issue. As a workaround, use modern drawing paths (e.g. `/rfx` or `/gfx` options). The workaround requires server side support. | 8.1 | More Details |
| CVE-2023-5397 | Server receiving a malformed message to create a new connection could lead to an attacker performing remote code execution or causing a failure. See Honeywell Security Notification for recommendations on upgrading and versioning. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-1132 | A flaw was found in Keycloak, where it does not properly validate URLs included in a redirect. This issue could allow an attacker to construct a malicious request to bypass validation and access other URLs and sensitive information within the domain or conduct further attacks. This flaw affects any client that utilizes a wildcard in the Valid Redirect URIs field, and requires user interaction within the malicious URL. | 8.1 | More Details |
| CVE-2023-4234 | A flaw was found in ofono, an Open Source Telephony on Linux. A stack overflow bug is triggered within the decode_submit_report() function during the SMS decoding. It is assumed that the attack scenario is accessible from a compromised modem, a malicious base station, or just SMS. There is a bound check for this memcpy length in decode_submit(), but it was forgotten in decode_submit_report(). | 8.1 | More Details |
| CVE-2024-30928 | SQL Injection vulnerability in DerbyNet v9.0 and below allows attackers to execute arbitrary SQL commands via 'classids' Parameter in ajax/query.slide.next.inc | 8.1 | More Details |
| CVE-2023-5395 | Server receiving a malformed message that uses the hostname in an internal table may cause a stack overflow resulting in possible remote code execution. See Honeywell Security Notification for recommendations on upgrading and versioning. | 8.1 | More Details |
| CVE-2024-21989 | ONTAP Select Deploy administration utility versions 9.12.1.x, 9.13.1.x and 9.14.1.x are susceptible to a vulnerability which when successfully exploited could allow a read-only user to escalate their privileges. | 8.1 | More Details |
| CVE-2023-4233 | A flaw was found in ofono, an Open Source Telephony on Linux. A stack overflow bug is triggered within the sms_decode_address_field() function during the SMS PDU decoding. It is assumed that the attack scenario is accessible from a compromised modem, a malicious base station, or just SMS. | 8.1 | More Details |
| CVE-2023-4235 | A flaw was found in ofono, an Open Source Telephony on Linux. A stack overflow bug is triggered within the decode_deliver_report() function during the SMS decoding. It is assumed that the attack scenario is accessible from a compromised modem, a malicious base station, or just SMS. There is a bound check for this memcpy length in decode_submit(), but it was forgotten in decode_deliver_report(). | 8.1 | More Details |
| CVE-2023-5401 | Server receiving a malformed message based on a using the specified key values can cause a stack overflow vulnerability which could lead to an attacker performing remote code execution or causing a failure. See Honeywell Security Notification for recommendations on upgrading and versioning. | 8.1 | More Details |
| CVE-2023-5403 | Server hostname translation to IP address manipulation which could lead to an attacker performing remote code execution or causing a failure. See Honeywell Security Notification for recommendations on upgrading and versioning. | 8.1 | More Details |
| CVE-2023-5404 | Server receiving a malformed message can cause a pointer to be overwritten which can result in a remote code execution or failure. See Honeywell Security Notification for recommendations on upgrading and versioning. | 8.1 | More Details |
| CVE-2023-4232 | A flaw was found in ofono, an Open Source Telephony on Linux. A stack overflow bug is triggered within the decode_status_report() function during the SMS decoding. It is assumed that the attack scenario is accessible from a compromised modem, a malicious base station, or just SMS. There is a bound check for this memcpy length in decode_submit(), but it was forgotten in decode_status_report(). | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-5400 | Server receiving a malformed message based on a using the specified key values can cause a heap overflow vulnerability which could lead to an attacker performing remote code execution or causing a failure.  See Honeywell Security Notification for recommendations on upgrading and versioning. | 8.1 | More Details |
| CVE-2024-32040 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients that use a version of FreeRDP prior to 3.5.0 or 2.11.6 and have connections to servers using the `NSC` codec are vulnerable to integer underflow. Versions 3.5.0 and 2.11.6 patch the issue. As a workaround, do not use the NSC codec (e.g. use `-nsc`). | 8.1 | More Details |
| CVE-2024-32303 | Tenda AC15 v15.03.20_multi, v15.03.05.19, and v15.03.05.18 firmware has a stack overflow vulnerability located via the PPW parameter in the fromWizardHandle function. | 8.0 | More Details |
| CVE-2024-32293 | Tenda W30E v1.0 V1.0.1.25(633) firmware has a stack overflow vulnerability via the page parameter in the fromDhcpListClient function. | 8.0 | More Details |
| CVE-2024-3646 | A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the instance when configuring the chat integration. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.12.2, 3.11.8, 3.10.10, and 3.9.13. This vulnerability was reported via the GitHub Bug Bounty program. | 8.0 | More Details |
| CVE-2024-3684 | A server side request forgery vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin access to the appliance when configuring the Artifacts & Logs and Migrations Storage. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.12.2, 3.11.8, 3.10.10, and 3.9.13. This vulnerability was reported via the GitHub Bug Bounty program. | 8.0 | More Details |
| CVE-2023-50009 | Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the ff_gaussian_blur_8 function in libavfilter/edge_template.c:116:5 component. | 8.0 | More Details |
| CVE-2024-32310 | Tenda F1203 V2.0.1.6 firmware has a stack overflow vulnerability located in the PPW parameter of the fromWizardHandle function. | 8.0 | More Details |
| CVE-2024-30929 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows attackers to execute arbitrary code via the 'back' Parameter in playlist.php | 8.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-38296 | Various software builds for the following TCL 30Z and TCL A3X devices leak the ICCID to a system property that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in these instances they are leaked by a high-privilege process and can be obtained indirectly. The software build fingerprints for each confirmed vulnerable device are as follows: TCL 30Z (TCL/4188R/Jetta_ATT:12/SP1A.210812.016/LV8E:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU5P:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU61:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU66:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU68:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU6P:user/release-keys, and TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU6X:user/release-keys) and TCL A3X (TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAAZ:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAB3:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAB7:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABA:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABM:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABP:user/release-keys, and TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABS:user/release-keys). This malicious app reads from the "persist.sys.tctPowerIccid" system property to indirectly obtain the ICCID. | 8.0 | More Details |
| CVE-2024-32285 | Tenda W30E v1.0 V1.0.1.25(633) firmware has a stack overflow vulnerability via the password parameter in the formaddUserName function. | 8.0 | More Details |
| CVE-2023-49501 | Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the config_eq_output function in the libavfilter/asrc_afirsrc.c:495:30 component. | 8.0 | More Details |
| CVE-2023-51795 | Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showspectrum.c:1789:52 component in showspectrumpic_request_frame | 8.0 | More Details |
| CVE-2023-51793 | Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavutil/imgutils.c:353:9 in image_copy_plane. | 7.8 | More Details |
| CVE-2023-51798 | Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via a floating point exception (FPE) error at libavfilter/vf_minterpolate.c:1078:60 in interpolate. | 7.8 | More Details |
| CVE-2023-51791 | Buffer Overflow vulenrability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavcodec/jpegxl_parser.c in gen_alias_map. | 7.8 | More Details |
| CVE-2023-50010 | Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the set_encoder_id function in /fftools/ffmpeg_enc.c component. | 7.8 | More Details |
| CVE-2023-50008 | Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via the av_malloc function in libavutil/mem.c:105:9 component. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26852 | In the Linux kernel, the following vulnerability has been resolved: net/ipv6: avoid possible UAF in ip6_route_mpath_notify() syzbot found another use-after-free in ip6_route_mpath_notify() [1] Commit f7225172f25a ("net/ipv6: prevent use after free in ip6_route_mpath_notify") was not able to fix the root cause. We need to defer the fib6_info_release() calls after ip6_route_mpath_notify(), in the cleanup phase. [1] BUG: KASAN: slab-use-after-free in rt6_fill_node+0x1460/0x1ac0 Read of size 4 at addr ffff88809a07fc64 by task syz-executor.2/23037 CPU: 0 PID: 23037 Comm: syz-executor.2 Not tainted 6.8.0-rc4-syzkaller-01035-gea7f3cfaa588 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/25/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1e7/0x2e0 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:377 [inline] print_report+0x167/0x540 mm/kasan/report.c:488 kasan_report+0x142/0x180 mm/kasan/report.c:601 rt6_fill_node+0x1460/0x1ac0 inet6_rt_notify+0x13b/0x290 net/ipv6/route.c:6184 ip6_route_mpath_notify net/ipv6/route.c:5198 [inline] ip6_route_multipath_add net/ipv6/route.c:5404 [inline] inet6_rtm_newroute+0x1d0f/0x2300 net/ipv6/route.c:5517 rtnetlink_rcv_msg+0x885/0x1040 net/core/rtnetlink.c:6597 netlink_rcv_skb+0x1e3/0x430 net/netlink/af_netlink.c:2543 netlink_unicast_kernel net/netlink/af_netlink.c:1341 [inline] netlink_unicast+0x7ea/0x980 net/netlink/af_netlink.c:1367 netlink_sendmsg+0xa3b/0xd70 net/netlink/af_netlink.c:1908 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x221/0x270 net/socket.c:745 ____sys_sendmsg+0x525/0x7d0 net/socket.c:2584 ___sys_sendmsg net/socket.c:2638 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2667 do_syscall_64+0xf9/0x240 entry_SYSCALL_64_after_hwframe+0x6f/0x77 RIP: 0033:0x7f73dd87dda9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 e1 20 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f73de6550c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f73dd9ac050 RCX: 00007f73dd87dda9 RDX: 0000000000000000 RSI: 0000000020000140 RDI: 0000000000000005 RBP: 00007f73dd8ca47a R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000006e R14: 00007f73dd9ac050 R15: 00007ffdbdeb7858 </TASK> Allocated by task 23037: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:372 [inline] __kasan_kmalloc+0x98/0xb0 mm/kasan/common.c:389 kasan_kmalloc include/linux/kasan.h:211 [inline] __do_kmalloc_node mm/slub.c:3981 [inline] __kmalloc+0x22e/0x490 mm/slub.c:3994 kmalloc include/linux/slab.h:594 [inline] kzalloc include/linux/slab.h:711 [inline] fib6_info_alloc+0x2e/0xf0 net/ipv6/ip6_fib.c:155 ip6_route_info_create+0x445/0x12b0 net/ipv6/route.c:3758 ip6_route_multipath_add net/ipv6/route.c:5298 [inline] inet6_rtm_newroute+0x744/0x2300 net/ipv6/route.c:5517 rtnetlink_rcv_msg+0x885/0x1040 net/core/rtnetlink.c:6597 netlink_rcv_skb+0x1e3/0x430 net/netlink/af_netlink.c:2543 netlink_unicast_kernel net/netlink/af_netlink.c:1341 [inline] netlink_unicast+0x7ea/0x980 net/netlink/af_netlink.c:1367 netlink_sendmsg+0xa3b/0xd70 net/netlink/af_netlink.c:1908 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x221/0x270 net/socket.c:745 ____sys_sendmsg+0x525/0x7d0 net/socket.c:2584 ___sys_sendmsg net/socket.c:2638 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2667 do_syscall_64+0xf9/0x240 entry_SYSCALL_64_after_hwframe+0x6f/0x77 Freed by task 16: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x4e/0x60 mm/kasan/generic.c:640 poison_slab_object+0xa6/0xe0 m ---truncated--- | 7.8 | More Details |
| CVE-2023-37400 | IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to escalate their privileges due to insecure credential storage. IBM X-Force ID: 259677. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-28699 | A buffer overflow vulnerability in pdf2json v0.70 allows a local attacker to execute arbitrary code via the GString::copy() and ImgOutputDev::ImgOutputDev function. | 7.8 | More Details |
| CVE-2024-26898 | In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts This patch is against CVE-2023-6270. The description of cve is: A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition or potential code execution. In aoecmd_cfg_pkts(), it always calls dev_put(ifp) when skb initial code is finished. But the net_device ifp will still be used in later tx()->dev_queue_xmit() in kthread. Which means that the dev_put(ifp) should NOT be called in the success path of skb initial code in aoecmd_cfg_pkts(). Otherwise tx() may run into use-after-free because the net_device is freed. This patch removed the dev_put(ifp) in the success path in aoecmd_cfg_pkts(), and added dev_put() after skb xmit in tx(). | 7.8 | More Details |
| CVE-2024-26913 | In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix dcn35 8k30 Underflow/Corruption Issue [why] odm calculation is missing for pipe split policy determination and cause Underflow/Corruption issue. [how] Add the odm calculation. | 7.8 | More Details |
| CVE-2023-38295 | Certain software builds for the TCL 30Z and TCL 10 Android devices contain a vulnerable, pre-installed app that relies on a missing permission that provides no protection at runtime. The missing permission is required as an access permission by components in various pre-installed apps. On the TCL 30Z device, the vulnerable app has a package name of com.tcl.screenrecorder (versionCode='1221092802', versionName='v5.2120.02.12008.1.T' ; versionCode='1221092805', versionName='v5.2120.02.12008.2.T'). On the TCL 10L device, the vulnerable app has a package name of com.tcl.sos (versionCode='2020102827', versionName='v3.2014.12.1012.B'). When a third-party app declares and requests the missing permission, it can interact with certain service components in the aforementioned apps (that execute with "system" privileges) to perform arbitrary files reads/writes in its context. An app exploiting this vulnerability only needs to declare and request the single missing permission and no user interaction is required beyond installing and running a third-party app. The software build fingerprints for each confirmed vulnerable device are as follows: TCL 10L (TCL/T770B/T1_LITE:11/RKQ1.210107.001/8BIC:user/release-keys) and TCL 30Z (TCL/4188R/Jetta_ATT:12/SP1A.210812.016/LV8E:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU5P:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU61:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU66:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU68:user/release-keys, TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU6P:user/release-keys, and TCL/T602DL/Jetta_TF:12/SP1A.210812.016/vU6X:user/release-keys). This malicious app declares the missing permission named com.tct.smart.switchphone.permission.SWITCH_DATA as a normal permission, requests the missing permission, and uses it to interact with the com.tct.smart.switchdata.DataService service component that is declared in vulnerable apps that execute with "system" privileges to perform arbitrary file reads/writes. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26907 | In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ------------[ cut here ]------------ memcpy: detected field-spanning write (size 56) of single field "eseg->inline_hdr.start" at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 (size 2) WARNING: CPU: 0 PID: 293779 at /var/lib/dkms/mlnx-ofed-kernel/5.8/build/drivers/infiniband/hw/mlx5/wr.c:131 mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] Modules linked in: 8021q garp mrp stp llc rdma_ucm(OE) rdma_cm(OE) iw_cm(OE) ib_ipoib(OE) ib_cm(OE) ib_umad(OE) mlx5_ib(OE) ib_uverbs(OE) ib_core(OE) mlx5_core(OE) pci_hyperv_intf mlxdevm(OE) mlx_compat(OE) tls mlxfw(OE) psample nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip_set nf_tables libcrc32c nfnetlink mst_pciconf(OE) knem(OE) vfio_pci vfio_pci_core vfio_iommu_type1 vfio iommufd irqbypass cuse nfsv3 nfs fscache netfs xfrm_user xfrm_algo ipmi_devintf ipmi_msghandler binfmt_misc crct10dif_pclmul crc32_pclmul polyval_clmulni polyval_generic ghash_clmulni_intel sha512_ssse3 snd_pcsp aesni_intel crypto_simd cryptd snd_pcm snd_timer joydev snd soundcore input_leds serio_raw evbug nfsd auth_rpcgss nfs_acl lockd grace sch_fq_codel sunrpc drm efi_pstore ip_tables x_tables autofs4 psmouse virtio_net net_failover failover floppy [last unloaded: mlx_compat(OE)] CPU: 0 PID: 293779 Comm: ssh Tainted: G OE 6.2.0-32-generic #32~22.04.1-Ubuntu Hardware name: Red Hat KVM, BIOS 0.5.1 01/01/2011 RIP: 0010:mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] Code: 0c 01 00 a8 01 75 25 48 8b 75 a0 b9 02 00 00 00 48 c7 c2 10 5b fd c0 48 c7 c7 80 5b fd c0 c6 05 57 0c 03 00 01 e8 95 4d 93 da <0f> 0b 44 8b 4d b0 4c 8b 45 c8 48 8b 4d c0 e9 49 fb ff ff 41 0f b7 RSP: 0018:ffffb5b48478b570 EFLAGS: 00010046 RAX: 0000000000000000 RBX: 0000000000000001 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffb5b48478b628 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffb5b48478b5e8 R13: ffff963a3c609b5e R14: ffff9639c3fbd800 R15: ffffb5b480475a80 FS: 00007fc03b444c80(0000) GS:ffff963a3dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000556f46bdf000 CR3: 0000000006ac6003 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? show_regs+0x72/0x90 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? __warn+0x8d/0x160 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] ? report_bug+0x1bb/0x1d0 ? handle_bug+0x46/0x90 ? exc_invalid_op+0x19/0x80 ? asm_exc_invalid_op+0x1b/0x20 ? mlx5_ib_post_send+0x191b/0x1a60 [mlx5_ib] mlx5_ib_post_send_nodrain+0xb/0x20 [mlx5_ib] ipoib_send+0x2ec/0x770 [ib_ipoib] ipoib_start_xmit+0x5a0/0x770 [ib_ipoib] dev_hard_start_xmit+0x8e/0x1e0 ? validate_xmit_skb_list+0x4d/0x80 sch_direct_xmit+0x116/0x3a0 __dev_xmit_skb+0x1fd/0x580 __dev_queue_xmit+0x284/0x6b0 ? _raw_spin_unlock_irq+0xe/0x50 ? __flush_work.isra.0+0x20d/0x370 ? push_pseudo_header+0x17/0x40 [ib_ipoib] neigh_connected_output+0xcd/0x110 ip_finish_output2+0x179/0x480 ? __smp_call_single_queue+0x61/0xa0 __ip_finish_output+0xc3/0x190 ip_finish_output+0x2e/0xf0 ip_output+0x78/0x110 ? __pfx_ip_finish_output+0x10/0x10 ip_local_out+0x64/0x70 __ip_queue_xmit+0x18a/0x460 ip_queue_xmit+0x15/0x30 __tcp_transmit_skb+0x914/0x9c0 tcp_write_xmit+0x334/0x8d0 tcp_push_one+0x3c/0x60 tcp_sendmsg_locked+0x2e1/0xac0 tcp_sendmsg+0x2d/0x50 inet_sendmsg+0x43/0x90 sock_sendmsg+0x68/0x80 sock_write_iter+0x93/0x100 vfs_write+0x326/0x3c0 ksys_write+0xbd/0xf0 ? do_syscall_64+0x69/0x90 __x64_sys_write+0x19/0x30 do_syscall_ ---truncated--- | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26884 | In the Linux kernel, the following vulnerability has been resolved: bpf: Fix hashtab overflow check on 32-bit arches The hashtab code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself can overflow by doing a 32-bit left-shift of an unsigned long value, which is undefined behaviour, so it is not guaranteed to truncate neatly. This was triggered by syzbot on the DEVMAP_HASH type, which contains the same check, copied from the hashtab code. So apply the same fix to hashtab, by moving the overflow check to before the roundup. | 7.8 | More Details |
| CVE-2023-38290 | Certain software builds for the BLU View 2 and Sharp Rouvo V Android devices contain a vulnerable pre-installed app with a package name of com.evenwell.fqc (versionCode='9020801', versionName='9.0208.01' ; versionCode='9020913', versionName='9.0209.13' ; versionCode='9021203', versionName='9.0212.03') that allows local third-party apps to execute arbitrary shell commands in its context (system user) due to inadequate access control. No permissions or special privileges are necessary to exploit the vulnerability in the com.evenwell.fqc app. No user interaction is required beyond installing and running a third-party app. The vulnerability allows local apps to access sensitive functionality that is generally restricted to pre-installed apps, such as programmatically performing the following actions: granting arbitrary permissions (which can be used to obtain sensitive user data), installing arbitrary apps, video recording the screen, wiping the device (removing the user's apps and data), injecting arbitrary input events, calling emergency phone numbers, disabling apps, accessing notifications, and much more. The software build fingerprints for each confirmed vulnerable device are as follows: BLU View 2 (BLU/B131DL/B130DL:11/RP1A.200720.011/1672046950:user/release-keys, BLU/B131DL/B130DL:11/RP1A.200720.011/1663816427:user/release-keys, BLU/B131DL/B130DL:11/RP1A.200720.011/1656476696:user/release-keys, BLU/B131DL/B130DL:11/RP1A.200720.011/1647856638:user/release-keys) and Sharp Rouvo V (SHARP/VZW_STTM21VAPP/STTM21VAPP:12/SP1A.210812.016/1KN0_0_460:user/release-keys and SHARP/VZW_STTM21VAPP/STTM21VAPP:12/SP1A.210812.016/1KN0_0_530:user/release-keys). This malicious app starts an exported activity named com.evenwell.fqc/.activity.ClickTest, crashes the com.evenwell.fqc app by sending an empty Intent (i.e., having not extras) to the com.evenwell.fqc/.FQCBroadcastReceiver receiver component, and then it sends command arbitrary shell commands to the com.evenwell.fqc/.FQCService service component which executes them with "system" privileges. | 7.8 | More Details |
| CVE-2024-31582 | FFmpeg version n6.1 was discovered to contain a heap buffer overflow vulnerability in the draw_block_rectangle function of libavfilter/vf_codecview.c. This vulnerability allows attackers to cause undefined behavior or a Denial of Service (DoS) via crafted input. | 7.8 | More Details |
| CVE-2024-26883 | In the Linux kernel, the following vulnerability has been resolved: bpf: Fix stackmap overflow check on 32-bit arches The stackmap code relies on roundup_pow_of_two() to compute the number of hash buckets, and contains an overflow check by checking if the resulting value is 0. However, on 32-bit arches, the roundup code itself can overflow by doing a 32-bit left-shift of an unsigned long value, which is undefined behaviour, so it is not guaranteed to truncate neatly. This was triggered by syzbot on the DEVMAP_HASH type, which contains the same check, copied from the hashtab code. The commit in the fixes tag actually attempted to fix this, but the fix did not account for the UB, so the fix only works on CPUs where an overflow does result in a neat truncation to zero, which is not guaranteed. Checking the value before rounding does not have this problem. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26885 | In the Linux kernel, the following vulnerability has been resolved: bpf: Fix DEVMAP_HASH overflow check on 32-bit arches The devmap code allocates a number hash buckets equal to the next power of two of the max_entries value provided when creating the map. When rounding up to the next power of two, the 32-bit variable storing the number of buckets can overflow, and the code checks for overflow by checking if the truncated 32-bit value is equal to 0. However, on 32-bit arches the rounding up itself can overflow mid-way through, because it ends up doing a left-shift of 32 bits on an unsigned long value. If the size of an unsigned long is four bytes, this is undefined behaviour, so there is no guarantee that we'll end up with a nice and tidy 0-value at the end. Syzbot managed to turn this into a crash on arm32 by creating a DEVMAP_HASH with max_entries > 0x80000000 and then trying to update it. Fix this by moving the overflow check to before the rounding up operation. | 7.8 | More Details |
| CVE-2024-31583 | Pytorch before version v2.2.0 was discovered to contain a use-after-free vulnerability in torch/csrc/jit/mobile/interpreter.cpp. | 7.8 | More Details |
| CVE-2024-32656 | Ant Media Server is live streaming engine software. A local privilege escalation vulnerability in present in versions 2.6.0 through 2.8.2 allows any unprivileged operating system user account to escalate privileges to the root user account on the system. This vulnerability arises from Ant Media Server running with Java Management Extensions (JMX) enabled and authentication disabled on localhost on port 5599/TCP. This vulnerability is nearly identical to the local privilege escalation vulnerability CVE-2023-26269 identified in Apache James. Any unprivileged operating system user can connect to the JMX service running on port 5599/TCP on localhost and leverage the MLet Bean within JMX to load a remote MBean from an attacker-controlled server. This allows an attacker to execute arbitrary code within the Java process run by Ant Media Server and execute code within the context of the `antmedia` service account on the system. Version 2.9.0 contains a patch for the issue. As a workaround, one may remove certain parameters from the `antmedia.service` file. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26882 | In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") 1ca1ba465e55 ("geneve: make sure to pull inner header in geneve_rx()") We have to save skb->network_header in a temporary variable in order to be able to recompute the network_header pointer after a pskb_inet_may_pull() call. pskb_inet_may_pull() makes sure the needed headers are in skb->head. syzbot reported: BUG: KMSAN: uninit-value in __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline] BUG: KMSAN: uninit-value in INET_ECN_decapsulate include/net/inet_ecn.h:275 [inline] BUG: KMSAN: uninit-value in IP_ECN_decapsulate include/net/inet_ecn.h:302 [inline] BUG: KMSAN: uninit-value in ip_tunnel_rcv+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline] INET_ECN_decapsulate include/net/inet_ecn.h:275 [inline] IP_ECN_decapsulate include/net/inet_ecn.h:302 [inline] ip_tunnel_rcv+0xed9/0x2ed0 net/ipv4/ip_tunnel.c:409 __ipgre_rcv+0x9bc/0xbc0 net/ipv4/ip_gre.c:389 ipgre_rcv net/ipv4/ip_gre.c:411 [inline] gre_rcv+0x423/0x19f0 net/ipv4/ip_gre.c:447 gre_rcv+0x2a4/0x390 net/ipv4/gre_demux.c:163 ip_protocol_deliver_rcu+0x264/0x1300 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x2b8/0x440 net/ipv4/ip_input.c:233 NF_HOOK include/linux/netfilter.h:314 [inline] ip_local_deliver+0x21f/0x490 net/ipv4/ip_input.c:254 dst_input include/net/dst.h:461 [inline] ip_rcv_finish net/ipv4/ip_input.c:449 [inline] NF_HOOK include/linux/netfilter.h:314 [inline] ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569 __netif_receive_skb_one_core net/core/dev.c:5534 [inline] __netif_receive_skb+0x1a6/0x5a0 net/core/dev.c:5648 netif_receive_skb_internal net/core/dev.c:5734 [inline] netif_receive_skb+0x58/0x660 net/core/dev.c:5793 tun_rx_batched+0x3ee/0x980 drivers/net/tun.c:1556 tun_get_user+0x53b9/0x66e0 drivers/net/tun.c:2009 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087 [inline] new_sync_write fs/read_write.c:497 [inline] vfs_write+0xb6b/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 fs/read_write.c:643 __do_sys_write fs/read_write.c:655 [inline] __se_sys_write fs/read_write.c:652 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 alloc_pages_mpol+0x62b/0x9d0 mm/mempolicy.c:2133 alloc_pages+0x1be/0x1e0 mm/mempolicy.c:2204 skb_page_frag_refill+0x2bf/0x7c0 net/core/sock.c:2909 tun_build_skb drivers/net/tun.c:1686 [inline] tun_get_user+0xe0a/0x66e0 drivers/net/tun.c:1826 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2055 call_write_iter include/linux/fs.h:2087 [inline] new_sync_write fs/read_write.c:497 [inline] vfs_write+0xb6b/0x1520 fs/read_write.c:590 ksys_write+0x20f/0x4c0 fs/read_write.c:643 __do_sys_write fs/read_write.c:655 [inline] __se_sys_write fs/read_write.c:652 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b | 7.8 | More Details |
| CVE-2024-29968 | An information disclosure vulnerability exists in Brocade SANnav before v2.3.1 and v2.3.0a when Brocade SANnav instances are configured in disaster recovery mode. SQL Table names, column names, and SQL queries are collected in DR standby Supportsave. This could allow authenticated users to access the database structure and its contents. | 7.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32477 | Deno is a JavaScript, TypeScript, and WebAssembly runtime with secure defaults. By using ANSI escape sequences and a race between `libc::tcflush(0, libc::TCIFLUSH)` and reading standard input, it's possible to manipulate the permission prompt and force it to allow an unsafe action regardless of the user input. Some ANSI escape sequences act as a info request to the master terminal emulator and the terminal emulator sends back the reply in the PTY channel. standard streams also use this channel to send and get data. For example the `\033[6n` sequence requests the current cursor position. These sequences allow us to append data to the standard input of Deno. This vulnerability allows an attacker to bypass Deno permission policy. This vulnerability is fixed in 1.42.2. | 7.7 | More Details |
| CVE-2023-51500 | Missing Authorization vulnerability in Undsgn Uncode Core.This issue affects Uncode Core: from n/a through 2.8.8. | 7.7 | More Details |
| CVE-2023-51418 | Missing Authorization vulnerability in Joris van Montfort JVM rich text icons.This issue affects JVM rich text icons: from n/a through 1.2.6. | 7.7 | More Details |
| CVE-2024-32602 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in OnTheGoSystems WooCommerce Multilingual & Multicurrency.This issue affects WooCommerce Multilingual & Multicurrency: from n/a through 5.3.3.1. | 7.6 | More Details |
| CVE-2024-32399 | Directory Traversal vulnerability in RaidenMAILD Mail Server v.4.9.4 and before allows a remote attacker to obtain sensitive information via the /webeditor/ component. | 7.6 | More Details |
| CVE-2024-32551 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Smartypants SP Project & Document Manager.This issue affects SP Project & Document Manager : from n/a through 4.71. | 7.6 | More Details |
| CVE-2023-47843 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Zachary Segal CataBlog.This issue affects CataBlog: from n/a through 1.7.0. | 7.6 | More Details |
| CVE-2024-32693 | Cross-Site Request Forgery (CSRF) vulnerability in ValvePress Automatic.This issue affects Automatic: from n/a before 3.93.0. | 7.6 | More Details |
| CVE-2024-29958 | A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a prints the encryption key in the console when a privileged user executes the script to replace the Brocade SANnav Management Portal standby node. This could provide attackers an additional, less protected path to acquiring the encryption key. | 7.5 | More Details |
| CVE-2024-31846 | An issue was discovered in Italtel Embrace 1.6.4. The web application does not restrict or incorrectly restricts access to a resource from an unauthorized actor. | 7.5 | More Details |
| CVE-2024-22179 | The application is vulnerable to an unauthenticated parameter manipulation that allows an attacker to set the credentials to blank giving her access to the admin panel. Also vulnerable to account takeover and arbitrary password change. | 7.5 | More Details |
| CVE-2024-3742 | Electrolink transmitters store credentials in clear-text. Use of these credentials could allow an attacker to access the system. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-22640 | TCPDF version <=6.6.5 is vulnerable to ReDoS (Regular Expression Denial of Service) if parsing an untrusted HTML page with a crafted color. | 7.5 | More Details |
| CVE-2024-29966 | Brocade SANnav OVA before v2.3.1 and v2.3.0a contain hard-coded credentials in the documentation that appear as the appliance's root password. The vulnerability could allow an unauthenticated attacker full access to the Brocade SANnav appliance. | 7.5 | More Details |
| CVE-2024-29969 | When a Brocade SANnav installation is upgraded from Brocade SANnav v2.2.2 to Brocade SANnav 2.3.0, TLS/SSL weak message authentication code ciphers are added by default for port 18082. | 7.5 | More Details |
| CVE-2024-3741 | Electrolink transmitters are vulnerable to an authentication bypass vulnerability affecting the login cookie. An attacker can set an arbitrary value except 'NO' to the login cookie and have full system access. | 7.5 | More Details |
| CVE-2024-31744 | In Jasper 4.2.2, the jpc_streamlist_remove function in src/libjasper/jpc/jpc_dec.c:2407 has an assertion failure vulnerability, allowing attackers to cause a denial of service attack through a specific image file. | 7.5 | More Details |
| CVE-2024-20380 | A vulnerability in the HTML parser of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an issue in the C to Rust foreign function interface. An attacker could exploit this vulnerability by submitting a crafted file containing HTML content to be scanned by ClamAV on an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software. | 7.5 | More Details |
| CVE-2024-1491 | The devices allow access to an unprotected endpoint that allows MPFS file system binary image upload without authentication. The MPFS2 file system module provides a light-weight read-only file system that can be stored in external EEPROM, external serial flash, or internal flash program memory. This file system serves as the basis for the HTTP2 web server module, but is also used by the SNMP module and is available to other applications that require basic read-only storage capabilities. This can be exploited to overwrite the flash program memory that holds the web server's main interfaces and execute arbitrary code. | 7.5 | More Details |
| CVE-2024-32475 | Envoy is a cloud-native, open source edge and service proxy. When an upstream TLS cluster is used with `auto_sni` enabled, a request containing a `host`/`:authority` header longer than 255 characters triggers an abnormal termination of Envoy process. Envoy does not gracefully handle an error when setting SNI for outbound TLS connection. The error can occur when Envoy attempts to use the `host`/`:authority` header value longer than 255 characters as SNI for outbound TLS connection. SNI length is limited to 255 characters per the standard. Envoy always expects this operation to succeed and abnormally aborts the process when it fails. This vulnerability is fixed in 1.30.1, 1.29.4, 1.28.3, and 1.27.5. | 7.5 | More Details |
| CVE-2024-29957 | When Brocade SANnav before v2.3.1 and v2.3.0a servers are configured in Disaster Recovery mode, the encryption key is stored in the DR log files. This could provide attackers with an additional, less-protected path to acquiring the encryption key. | 7.5 | More Details |
| CVE-2024-31841 | An issue was discovered in Italtel Embrace 1.6.4. The web server fails to sanitize input data, allowing remote unauthenticated attackers to read arbitrary files on the filesystem. | 7.5 | More Details |
| CVE-2024-21872 | The device allows an unauthenticated attacker to bypass authentication and modify the cookie to reveal hidden pages that allows more critical operations to the transmitter. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-31503 | Incorrect access control in Dolibarr ERP CRM versions 19.0.0 and before, allows authenticated attackers to steal victim users' session cookies and CSRF protection tokens via user interaction with a crafted web page, leading to account takeover. | 7.5 | More Details |
| CVE-2024-26854 | In the Linux kernel, the following vulnerability has been resolved: ice: fix uninitialized dplls mutex usage The pf->dplls.lock mutex is initialized too late, after its first use. Move it to the top of ice_dpll_init. Note that the "err_exit" error path destroys the mutex. And the mutex is the last thing destroyed in ice_dpll_deinit. This fixes the following warning with CONFIG_DEBUG_MUTEXES: ice 0000:10:00.0: The DDP package was successfully loaded: ICE OS Default Package version 1.3.36.0 ice 0000:10:00.0: 252.048 Gb/s available PCIe bandwidth (16.0 GT/s PCIe x16 link) ice 0000:10:00.0: PTP init successful ----------[ cut here ]---------- DEBUG_LOCKS_WARN_ON(lock->magic != lock) WARNING: CPU: 0 PID: 410 at kernel/locking/mutex.c:587 __mutex_lock+0x773/0xd40 Modules linked in: crct10dif_pclmul crc32_pclmul crc32c_intel polyval_clmulni polyval_generic ice(+) nvme nvme_c> CPU: 0 PID: 410 Comm: kworker/0:4 Not tainted 6.8.0-rc5+ #3 Hardware name: HPE ProLiant DL110 Gen10 Plus/ProLiant DL110 Gen10 Plus, BIOS U56 10/19/2023 Workqueue: events work_for_cpu_fn RIP: 0010:__mutex_lock+0x773/0xd40 Code: c0 0f 84 1d f9 ff ff 44 8b 35 0d 9c 69 01 45 85 f6 0f 85 0d f9 ff ff 48 c7 c6 12 a2 a9 85 48 c7 c7 12 f1 a> RSP: 0018:ff7eb1a3417a7ae0 EFLAGS: 00010286 RAX: 0000000000000000 RBX: 0000000000000002 RCX: 0000000000000000 RDX: 0000000000000002 RSI: ffffffff85ac2bff RDI: 00000000ffffffff RBP: ff7eb1a3417a7b80 R08: 0000000000000000 R09: 00000000ffffbfff R10: ff7eb1a3417a7978 R11: ff32b80f7fd2e568 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ff32b7f02c50e0d8 FS: 0000000000000000(0000) GS:ff32b80efe800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055b5852cc000 CR3: 000000003c43a004 CR4: 0000000000771ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __warn+0x84/0x170 ? __mutex_lock+0x773/0xd40 ? report_bug+0x1c7/0x1d0 ? prb_read_valid+0x1b/0x30 ? handle_bug+0x42/0x70 ? exc_invalid_op+0x18/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? __mutex_lock+0x773/0xd40 ? rcu_is_watching+0x11/0x50 ? __kmalloc_node_track_caller+0x346/0x490 ? ice_dpll_lock_status_get+0x28/0x50 [ice] ? __pfx_ice_dpll_lock_status_get+0x10/0x10 [ice] ? ice_dpll_lock_status_get+0x28/0x50 [ice] ice_dpll_lock_status_get+0x28/0x50 [ice] dpll_device_get_one+0x14f/0x2e0 dpll_device_event_send+0x7d/0x150 dpll_device_register+0x124/0x180 ice_dpll_init_dpll+0x7b/0xd0 [ice] ice_dpll_init+0x224/0xa40 [ice] ? _dev_info+0x70/0x90 ice_load+0x468/0x690 [ice] ice_probe+0x75b/0xa10 [ice] ? _raw_spin_unlock_irqrestore+0x4f/0x80 ? process_one_work+0x1a3/0x500 local_pci_probe+0x47/0xa0 work_for_cpu_fn+0x17/0x30 process_one_work+0x20d/0x500 worker_thread+0x1df/0x3e0 ? __pfx_worker_thread+0x10/0x10 kthread+0x103/0x140 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x31/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> irq event stamp: 125197 hardirqs last enabled at (125197): [<ffffffff8416409d>] finish_task_switch.isra.0+0x12d/0x3d0 hardirqs last disabled at (125196): [<ffffffff85134044>] __schedule+0xea4/0x19f0 softirqs last enabled at (105334): [<ffffffff84e1e65a>] napi_get_frags_check+0x1a/0x60 softirqs last disabled at (105332): [<ffffffff84e1e65a>] napi_get_frags_check+0x1a/0x60 ---[ end trace 0000000000000000 ]--- | 7.5 | More Details |
| CVE-2023-48183 | QuickJS before c4cdd61 has a build_for_in_iterator NULL pointer dereference because of an erroneous lexical scope of "this" with eval. | 7.5 | More Details |
| CVE-2024-29950 | The class FileTransfer implemented in Brocade SANnav before v2.3.1, v2.3.0a, uses the ssh-rsa signature scheme, which has a SHA-1 hash. The vulnerability could allow a remote, unauthenticated attacker to perform a man-in-the-middle attack. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3840 | Insufficient policy enforcement in Site Isolation in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) | 7.5 | More Details |
| CVE-2024-31031 | An issue in `coap_pdu.c` in libcoap 4.3.4 allows attackers to cause undefined behavior via a sequence of messages leading to unsigned integer overflow. | 7.5 | More Details |
| CVE-2024-2493 | Session Hijacking vulnerability in Hitachi Ops Center Analyzer.This issue affects Hitachi Ops Center Analyzer: from 10.0.0-00 before 11.0.1-00. | 7.5 | More Details |
| CVE-2024-31041 | Null Pointer Dereference vulnerability in topic_filtern function in mqtt_parser.c in NanoMQ 0.21.7 allows attackers to cause a denial of service. | 7.5 | More Details |
| CVE-2024-29001 | A SolarWinds Platform SWQL Injection Vulnerability was identified in the user interface. This vulnerability requires authentication and user interaction to be exploited. | 7.5 | More Details |
| CVE-2024-28627 | An issue in Flipsnack v.18/03/2024 allows a local attacker to obtain sensitive information via the reader.gz.js file. | 7.5 | More Details |
| CVE-2024-29003 | The SolarWinds Platform was susceptible to a XSS vulnerability that affects the maps section of the user interface. This vulnerability requires authentication and requires user interaction. | 7.5 | More Details |
| CVE-2024-28130 | An incorrect type conversion vulnerability exists in the DVPSSoftcopyVOI_PList::createFromImage functionality of OFFIS DCMTK 3.6.8. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. | 7.5 | More Details |
| CVE-2024-33214 | Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the entrys parameter in ip/goform/RouteStatic. | 7.5 | More Details |
| CVE-2024-33217 | Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the page parameter in ip/goform/addressNat. | 7.5 | More Details |
| CVE-2024-32660 | FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.5.1, a malicious server can crash the FreeRDP client by sending invalid huge allocation size. Version 3.5.1 contains a patch for the issue. No known workarounds are available. | 7.5 | More Details |
| CVE-2024-32661 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients prior to version 3.5.1 are vulnerable to a possible `NULL` access and crash. Version 3.5.1 contains a patch for the issue. No known workarounds are available. | 7.5 | More Details |
| CVE-2024-32662 | FreeRDP is a free implementation of the Remote Desktop Protocol. FreeRDP based clients prior to version 3.5.1 are vulnerable to out-of-bounds read. This occurs when `WCHAR` string is read with twice the size it has and converted to `UTF-8`, `base64` decoded. The string is only used to compare against the redirection server certificate. Version 3.5.1 contains a patch for the issue. No known workarounds are available. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32650 | Rustls is a modern TLS library written in Rust. `rustls::ConnectionCommon::complete_io` could fall into an infinite loop based on network input. When using a blocking rustls server, if a client send a `close_notify` message immediately after `client_hello`, the server's `complete_io` will get in an infinite loop. This vulnerability is fixed in 0.23.5, 0.22.4, and 0.21.11. | 7.5 | More Details |
| CVE-2024-32291 | Tenda W30E v1.0 firmware v1.0.1.25(633) has a stack overflow vulnerability via the page parameter in the fromNatlimit function. | 7.5 | More Details |
| CVE-2024-31578 | FFmpeg version n6.1.1 was discovered to contain a heap use-after-free via the av_hwframe_ctx_init function. | 7.5 | More Details |
| CVE-2024-1480 | Unitronics Vision Standard line of controllers allow the Information Mode password to be retrieved without authentication. | 7.5 | More Details |
| CVE-2023-44227 | Missing Authorization vulnerability in Mitchell Bennis Simple File List.This issue affects Simple File List: from n/a through 6.1.9. | 7.5 | More Details |
| CVE-2024-32652 | The adapter @hono/node-server allows you to run your Hono application on Node.js. Prior to 1.10.1, the application hangs when receiving a Host header with a value that `@hono/node-server` can't handle well. Invalid values are those that cannot be parsed by the `URL` as a hostname such as an empty string, slashes `/`, and other strings. The version 1.10.1 includes the fix for this issue. | 7.5 | More Details |
| CVE-2022-35503 | Improper verification of a user input in Open Source MANO v7-v12 allows an authenticated attacker to execute arbitrary code within the LCM module container via a Virtual Network Function (VNF) descriptor. An attacker may be able execute code to change the normal execution of the OSM components, retrieve confidential information, or gain access other parts of a Telco Operator infrastructure other than OSM itself. | 7.5 | More Details |
| CVE-2024-22808 | An issue in Tormach xsTECH CNC Router, PathPilot Controller v2.9.6 allows attackers to cause a Denial of Service (DoS) by disrupting the communication between the PathPilot controller and the CNC router via overwriting the card's name in the device memory. | 7.5 | More Details |
| CVE-2023-46060 | A Buffer Overflow vulnerability in Tenda AC500 v.2.0.1.9 allows a remote attacker to cause a denial of service via the port parameter at the goform/setVlanInfo component. | 7.5 | More Details |
| CVE-2024-30253 | @solana/web3.js is the Solana JavaScript SDK. Using particular inputs with `@solana/web3.js` will result in memory exhaustion (OOM). If you have a server, client, mobile, or desktop product that accepts untrusted input for use with `@solana/web3.js`, your application/service may crash, resulting in a loss of availability. This vulnerability is fixed in 1.0.1, 1.10.2, 1.11.1, 1.12.1, 1.1.2, 1.13.1, 1.14.1, 1.15.1, 1.16.2, 1.17.1, 1.18.1, 1.19.1, 1.20.3, 1.21.1, 1.22.1, 1.23.1, 1.24.3, 1.25.1, 1.26.1, 1.27.1, 1.28.1, 1.2.8, 1.29.4, 1.30.3, 1.31.1, 1.3.1, 1.32.3, 1.33.1, 1.34.1, 1.35.2, 1.36.1, 1.37.3, 1.38.1, 1.39.2, 1.40.2, 1.41.11, 1.4.1, 1.42.1, 1.43.7, 1.44.4, 1.45.1, 1.46.1, 1.47.5, 1.48.1, 1.49.1, 1.50.2, 1.51.1, 1.5.1, 1.52.1, 1.53.1, 1.54.2, 1.55.1, 1.56.3, 1.57.1, 1.58.1, 1.59.2, 1.60.1, 1.61.2, 1.6.1, 1.62.2, 1.63.2, 1.64.1, 1.65.1, 1.66.6, 1.67.3, 1.68.2, 1.69.1, 1.70.4, 1.71.1, 1.72.1, 1.7.2, 1.73.5, 1.74.1, 1.75.1, 1.76.1, 1.77.4, 1.78.8, 1.79.1, 1.80.1, 1.81.1, 1.8.1, 1.82.1, 1.83.1, 1.84.1, 1.85.1, 1.86.1, 1.87.7, 1.88.1, 1.89.2, 1.90.2, 1.9.2, and 1.91.3. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32317 | Tenda AC10 v4.0 V16.03.10.13 and V16.03.10.20 firmware has a stack overflow vulnerability via the adslPwd parameter in the formWanParameterSetting function. | 7.5 | More Details |
| CVE-2024-32307 | Tenda FH1205 V2.0.0.7(775) firmware has a stack overflow vulnerability located via the PPW parameter in the fromWizardHandle function. | 7.4 | More Details |
| CVE-2024-30920 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows a remote attacker to execute arbitrary code via the render-document.php component. | 7.4 | More Details |
| CVE-2024-1249 | A flaw was found in Keycloak's OIDC component in the "checkLoginIframe," which allows unvalidated cross-origin messages. This flaw allows attackers to coordinate and send millions of requests in seconds using simple code, significantly impacting the application's availability without proper origin validation for incoming messages. | 7.4 | More Details |
| CVE-2023-5396 | Server receiving a malformed message creates connection for a hostname that may cause a stack overflow resulting in possible remote code execution. See Honeywell Security Notification for recommendations on upgrading and versioning. | 7.4 | More Details |
| CVE-2024-33211 | Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the PPPOEPassword parameter in ip/goform/QuickIndex. | 7.3 | More Details |
| CVE-2024-32391 | Cross Site Scripting vulnerability in MacCMS v.10 v.2024.1000.3000 allows a remote attacker to execute arbitrary code via a crafted payload. | 7.3 | More Details |
| CVE-2024-32283 | Tenda FH1203 V2.0.1.6 firmware has a command injection vulnerablility in formexeCommand function via the cmdinput parameter. | 7.3 | More Details |
| CVE-2024-24910 | A local attacker can escalate privileges on affected Check Point ZoneAlarm Extreme Security NextGen, Identity Agent for Windows, and Identity Agent for Windows Terminal Server. To exploit this vulnerability, an attacker must first obtain the ability to execute local privileged code on the target system. | 7.3 | More Details |
| CVE-2024-30974 | SQL Injection vulnerability in autoexpress v.1.3.0 allows attackers to run arbitrary SQL commands via the carId parameter. | 7.3 | More Details |
| CVE-2024-32368 | Insecure Permission vulnerability in Agasta Sanketlife 2.0 Pocket 12-Lead ECG Monitor FW Version 3.0 allows a local attacker to cause a denial of service via the Bluetooth Low Energy (BLE) component. | 7.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-38293 | Certain software builds for the Nokia C200 and Nokia C100 Android devices contain a vulnerable, pre-installed app with a package name of com.tracfone.tfstatus (versionCode='31', versionName='12') that allows local third-party apps to execute arbitrary AT commands in its context (radio user) via AT command injection due to inadequate access control and inadequate input filtering. No permissions or special privileges are necessary to exploit the vulnerability in the com.tracfone.tfstatus app. No user interaction is required beyond installing and running a third-party app. The software build fingerprints for each confirmed vulnerable device are as follows: Nokia C200 (Nokia/Drake_02US/DRK:12/SP1A.210812.016/02US_1_080:user/release-keys and Nokia/Drake_02US/DRK:12/SP1A.210812.016/02US_1_040:user/release-keys) and Nokia C100 (Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_270:user/release-keys, Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_190:user/release-keys, Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_130:user/release-keys, Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_110:user/release-keys, Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_080:user/release-keys, and Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_050:user/release-keys). This malicious app sends a broadcast Intent to the receiver component named com.tracfone.tfstatus/.TFStatus. This broadcast receiver extracts a string from the Intent and uses it as an extra when it starts the com.tracfone.tfstatus/.TFStatusActivity activity component which uses the externally controlled string as an input to execute an AT command. There are two different injection techniques to successfully inject arbitrary AT commands to execute. | 7.3 | More Details |
| CVE-2024-32474 | Sentry is an error tracking and performance monitoring platform. Prior to 24.4.1, when authenticating as a superuser to Sentry with a username and password, the password is leaked as cleartext in logs under the _event_: `auth-index.validate_superuser`. An attacker with access to the log data could use these leaked credentials to login to the Sentry system as superuser. Self-hosted users on affected versions should upgrade to 24.4.1 or later. Users can configure the logging level to exclude logs of the `INFO` level and only generate logs for levels at `WARNING` or more. | 7.3 | More Details |
| CVE-2024-2961 | The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable. | 7.3 | More Details |
| CVE-2024-30983 | SQL Injection vulnerability in phpgurukul Cyber Cafe Management System Using PHP & MySQL 1.0 allows attackers to run arbitrary SQL commands via the compname parameter in /edit-computer-detail.php file. | 7.3 | More Details |
| CVE-2024-32345 | A cross-site scripting (XSS) vulnerability in the Settings menu of CMSimple v5.15 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Configuration parameter under the Language section. | 7.2 | More Details |
| CVE-2024-32480 | LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. Versions prior to 24.4.0 are vulnerable to SQL injection. The `order` parameter is obtained from `$request`. After performing a string check, the value is directly incorporated into an SQL statement and concatenated, resulting in a SQL injection vulnerability. An attacker may extract a whole database this way. Version 24.4.0 fixes the issue. | 7.2 | More Details |
| CVE-2024-3600 | The Poll Maker – Best WordPress Poll Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting due to a missing capability check on the ays_poll_maker_quick_start AJAX action in addition to insufficient escaping and sanitization in all versions up to, and including, 5.1.8. This makes it possible for unauthenticated attackers to create quizzes and inject malicious web scripts into them that execute when a user visits the page. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-31077 | Forminator prior to 1.29.3 contains a SQL injection vulnerability. If this vulnerability is exploited, a remote authenticated attacker with an administrative privilege may obtain and alter any information in the database and cause a denial-of-service (DoS) condition. | 7.2 | More Details |
| CVE-2024-32682 | Missing Authorization vulnerability in BdThemes Prime Slider – Addons For Elementor.This issue affects Prime Slider – Addons For Elementor: from n/a through 3.13.2. | 7.1 | More Details |
| CVE-2024-2419 | A flaw was found in Keycloak's redirect_uri validation logic. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to the theft of an access token, making it possible for the attacker to impersonate other users. It is very similar to CVE-2023-6291. | 7.1 | More Details |
| CVE-2024-32538 | Cross-Site Request Forgery (CSRF) vulnerability in Joshua Eldridge Easy CountDowner allows Stored XSS.This issue affects Easy CountDowner: from n/a through 1.0.8. | 7.1 | More Details |
| CVE-2024-32583 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Photo Gallery Team Photo Gallery by 10Web allows Reflected XSS.This issue affects Photo Gallery by 10Web: from n/a through 1.8.21. | 7.1 | More Details |
| CVE-2024-32694 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative interactive media 3D FlipBook, PDF Viewer, PDF Embedder – Real 3D FlipBook WordPress Plugin allows Reflected XSS.This issue affects 3D FlipBook, PDF Viewer, PDF Embedder – Real 3D FlipBook WordPress Plugin: from n/a through 3.62. | 7.1 | More Details |
| CVE-2024-32695 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marco Gasi Language Switcher for Transposh allows Reflected XSS.This issue affects Language Switcher for Transposh: from n/a through 1.5.9. | 7.1 | More Details |
| CVE-2024-32582 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bowo Debug Log Manager allows Stored XSS.This issue affects Debug Log Manager: from n/a through 2.3.1. | 7.1 | More Details |
| CVE-2024-32541 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tobias Battenberg WP-Cufon allows Stored XSS.This issue affects WP-Cufon: from n/a through 1.6.10. | 7.1 | More Details |
| CVE-2024-32542 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Organic Themes Bulk Block Converter allows Reflected XSS.This issue affects Bulk Block Converter: from n/a through 1.0.1. | 7.1 | More Details |
| CVE-2024-32543 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Minoji MJ Update History allows Reflected XSS.This issue affects MJ Update History: from n/a through 1.0.4. | 7.1 | More Details |
| CVE-2024-32544 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Netgsm allows Reflected XSS.This issue affects Netgsm: from n/a through 2.8. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32463 | phlex is an open source framework for building object-oriented views in Ruby. There is a potential cross-site scripting (XSS) vulnerability that can be exploited via maliciously crafted user data. The filter to detect and prevent the use of the `javascript:` URL scheme in the `href` attribute of an `<a>` tag could be bypassed with tab `\t` or newline `\n` characters between the characters of the protocol, e.g. `java\tscript:`. This vulnerability is fixed in 1.10.1, 1.9.2, 1.8.3, 1.7.2, 1.6.3, 1.5.3, and 1.4.2. Configuring a Content Security Policy that does not allow `unsafe-inline` would effectively prevent this vulnerability from being exploited. | 7.1 | More Details |
| CVE-2023-3758 | A race condition flaw was found in sssd where the GPO policy is not consistently applied for authenticated users. This may lead to improper authorization issues, granting or denying access to resources inappropriately. | 7.1 | More Details |
| CVE-2024-32585 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in extendWP Import Content in WordPress & WooCommerce with Excel allows Reflected XSS.This issue affects Import Content in WordPress & WooCommerce with Excel: from n/a through 4.2. | 7.1 | More Details |
| CVE-2024-32558 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode eCommerce Product Catalog allows Reflected XSS.This issue affects eCommerce Product Catalog: from n/a through 3.3.32. | 7.1 | More Details |
| CVE-2024-32545 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Canva Canva – Design beautiful blog graphics allows Reflected XSS.This issue affects Canva – Design beautiful blog graphics: from n/a through 1.2.4. | 7.1 | More Details |
| CVE-2024-32578 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 10Web Slider by 10Web allows Reflected XSS.This issue affects Slider by 10Web: from n/a through 1.2.54. | 7.1 | More Details |
| CVE-2024-32559 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hwk-fr WP 404 Auto Redirect to Similar Post allows Reflected XSS.This issue affects WP 404 Auto Redirect to Similar Post: from n/a through 1.0.4. | 7.1 | More Details |
| CVE-2024-32546 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Adam Bowen Tax Rate Upload allows Reflected XSS.This issue affects Tax Rate Upload: from n/a through 2.4.5. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-38291 | An issue was discovered in a third-party component related to ro.boot.wifimacaddr, shipped on devices from multiple device manufacturers. Various software builds for the following TCL devices (30Z and 10L) and Motorola devices (Moto G Pure and Moto G Power) leak the Wi-Fi MAC address to a system property that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in these instances they are leaked by a high-privilege process and can be obtained indirectly. The software build fingerprints for each confirmed vulnerable device are as follows: TCL A3X (TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAAZ:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAB3:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vAB7:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABA:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABM:user/release-keys, TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABP:user/release-keys, and TCL/A600DL/Delhi_TF:11/RKQ1.201202.002/vABS:user/release-keys); TCL 10L (TCL/T770B/T1_LITE:10/QKQ1.200329.002/3CJ0:user/release-keys and TCL/T770B/T1_LITE:11/RKQ1.210107.001/8BIC:user/release-keys); Motorola Moto G Pure (motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-2/74844:user/release-keys, motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-7/5cde8:user/release-keys, motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-10/d67faa:user/release-keys, motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-13/b4a29:user/release-keys, motorola/ellis_trac/ellis:12/S3RH32.20-42-10/1c2540:user/release-keys, motorola/ellis_trac/ellis:12/S3RHS32.20-42-13-2-1/6368dd:user/release-keys, motorola/ellis_a/ellis:11/RRH31.Q3-46-50-2/20fec:user/release-keys, motorola/ellis_vzw/ellis:11/RRH31.Q3-46-138/103bd:user/release-keys, motorola/ellis_vzw/ellis:11/RRHS31.Q3-46-138-2/e5502:user/release-keys, and motorola/ellis_vzw/ellis:12/S3RHS32.20-42-10-14-2/5e0b0:user/release-keys); and Motorola Moto G Power (motorola/tonga_g/tonga:11/RRQ31.Q3-68-16-2/e5877:user/release-keys and motorola/tonga_g/tonga:12/S3RQS32.20-42-10-6/f876d3:user/release-keys). This malicious app reads from the "ro.boot.wifimacaddr" system property to indirectly obtain the Wi-Fi MAC address. | 7.1 | More Details |
| CVE-2022-34560 | A cross-site scripting (XSS) vulnerability in PHPFox v4.8.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the History parameter. | 7.1 | More Details |
| CVE-2024-32563 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VikBooking Hotel Booking Engine & PMS allows Reflected XSS.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.6.7. | 7.1 | More Details |
| CVE-2024-32574 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ashish Ajani WP Simple HTML Sitemap allows Reflected XSS.This issue affects WP Simple HTML Sitemap: from n/a through 2.8. | 7.1 | More Details |
| CVE-2024-32567 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Designinvento DirectoryPress allows Reflected XSS.This issue affects DirectoryPress: from n/a through 3.6.7. | 7.1 | More Details |
| CVE-2024-32535 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jojaba Access Category Password allows Reflected XSS.This issue affects Access Category Password: from n/a through 1.5.1. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32533 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Peter Shaw LH Add Media From Url allows Reflected XSS.This issue affects LH Add Media From Url: from n/a through 1.22. | 7.1 | More Details |
| CVE-2024-32409 | An issue in SEMCMS v.4.8 allows a remote attacker to execute arbitrary code via a crafted script. | 7.1 | More Details |
| CVE-2024-32479 | LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. Prior to version 24.4.0, there is improper sanitization on the `Service` template name, which can lead to stored Cross-site Scripting. Version 24.4.0 fixes this vulnerability. | 7.1 | More Details |
| CVE-2024-32549 | Cross-Site Request Forgery (CSRF) vulnerability in Microkid Related Posts for WordPress allows Cross-Site Scripting (XSS).This issue affects Related Posts for WordPress: from n/a through 4.0.3. | 7.1 | More Details |
| CVE-2024-32550 | Cross-Site Request Forgery (CSRF) vulnerability in BMI Adult & Kid Calculator allows Stored XSS.This issue affects BMI Adult & Kid Calculator: from n/a through 1.2.1. | 7.1 | More Details |
| CVE-2024-32587 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EnvialoSimple EnvíaloSimple allows Reflected XSS.This issue affects EnvíaloSimple: from n/a through 2.2. | 7.1 | More Details |
| CVE-2024-32553 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in looks_awesome Superfly Menu allows Stored XSS.This issue affects Superfly Menu: from n/a through 5.0.25. | 7.1 | More Details |
| CVE-2024-32588 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress Export Import allows Reflected XSS.This issue affects LearnPress Export Import: from n/a through 4.0.3. | 7.1 | More Details |
| CVE-2024-32570 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Archetyped Cornerstone allows Reflected XSS.This issue affects Cornerstone: from n/a through 0.8.0. | 7.1 | More Details |
| CVE-2024-32595 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mat Bao Corp WP Helper Premium allows Reflected XSS.This issue affects WP Helper Premium: from n/a before 4.6.0. | 7.1 | More Details |
| CVE-2024-32568 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Melapress WP 2FA allows Reflected XSS.This issue affects WP 2FA: from n/a through 2.6.2. | 7.1 | More Details |
| CVE-2024-32461 | LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A SQL injection vulnerability in POST /search/search=packages in LibreNMS prior to version 24.4.0 allows a user with global read privileges to execute SQL commands via the package parameter. With this vulnerability, an attacker can exploit a SQL injection time based vulnerability to extract all data from the database, such as administrator credentials. Version 24.4.0 contains a patch for the vulnerability. | 7.1 | More Details |
| CVE-2024-32531 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Everest themes GuCherry Blog allows Reflected XSS.This issue affects GuCherry Blog: from n/a through 1.1.8. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32528 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Seerox WP Dynamic Keywords Injector allows Reflected XSS.This issue affects WP Dynamic Keywords Injector: from n/a through 2.3.18. | 7.1 | More Details |
| CVE-2024-32510 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Loopus WP Cost Estimation & Payment Forms Builder allows Reflected XSS.This issue affects WP Cost Estimation & Payment Forms Builder: from n/a through 10.1.75. | 7.1 | More Details |
| CVE-2024-31552 | CuteHttpFileServer v.3.1 version has an arbitrary file download vulnerability, which allows attackers to download arbitrary files on the server and obtain sensitive information. | 7.1 | More Details |
| CVE-2024-28076 | The SolarWinds Platform was susceptible to a Arbitrary Open Redirection Vulnerability. A potential attacker can redirect to different domain when using URL parameter with relative entry in the correct format | 7.0 | More Details |
| CVE-2024-22354 | IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.5 are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information, consume memory resources, or to conduct a server-side request forgery attack. IBM X-Force ID: 280401. | 7.0 | More Details |
| CVE-2024-22905 | Buffer Overflow vulnerability in ARM mbed-os v.6.17.0 allows a remote attacker to execute arbitrary code via a crafted script to the hciTrSerialRxIncoming function. | 7.0 | More Details |
| CVE-2024-32478 | Git Credential Manager (GCM) is a secure Git credential helper. Prior to 2.5.0, the Debian package does not set root ownership on installed files. This allows user 1001 on a multi-user system can replace binary and gain other users' privileges. This vulnerability is fixed in 2.5.0. | 6.9 | More Details |
| CVE-2024-30987 | Cross Site Scripting vulnerability in /bwdates-reports-ds.php of phpgurukul Client Management System using PHP & MySQL 1.1 allows attackers to execute arbitrary code and obtain sensitive information via the fromdate and todate parameters. | 6.8 | More Details |
| CVE-2024-30988 | Cross Site Scripting vulnerability in /search-invoices.php of phpgurukul Client Management System using PHP & MySQL 1.1 allows attackers to execute arbitrary code and obtain sensitive information via the Search bar. | 6.8 | More Details |
| CVE-2024-31036 | A heap-buffer-overflow vulnerability in the read_byte function in NanoMQ v.0.21.7 allows attackers to cause a denial of service via transmission of crafted hexstreams. | 6.8 | More Details |
| CVE-2023-36505 | Improper Input Validation vulnerability in Saturday Drive Ninja Forms Contact Form.This issue affects Ninja Forms Contact Form : from n/a through 3.6.24. | 6.8 | More Details |
| CVE-2024-3185 | A key used in logging.json does not follow the least privilege principle by default and is exposed to local users in the Rapid7 Platform. This allows an attacker with local access to a machine with the logging.json file to use that key to authenticate to the platform with high privileges. This was fixed in the Rapid7 platform starting 3 April 2024 via the introduction of a restricted role and the removal of automatic API key generation on installation of an agent. | 6.8 | More Details |
| CVE-2024-22440 | A potential security vulnerability has been identified in HPE Compute Scale-up Server 3200 server. This vulnerability could cause disclosure of sensitive information in log files. | 6.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-29960 | In Brocade SANnav server before v2.3.1 and v2.3.0a, the SSH keys inside the OVA image are identical in the VM every time SANnav is installed. Any Brocade SAnnav VM based on the official OVA images is vulnerable to MITM over SSH. An attacker can decrypt and compromise the SSH traffic to the SANnav. | 6.8 | More Details |
| CVE-2024-29965 | In Brocade SANnav before v2.3.1, and v2.3.0a, it is possible to back up the appliance from the web interface or the command line interface ("SSH"). The resulting backups are world-readable. A local attacker can recover backup files, restore them to a new malicious appliance, and retrieve the passwords of all the switches. | 6.8 | More Details |
| CVE-2024-32326 | TOTOLINK EX200 V4.0.3c.7646_B20201211 contains a Cross-site scripting (XSS) vulnerability through the key parameter in the setWiFiExtenderConfig function. | 6.8 | More Details |
| CVE-2023-40146 | A privilege escalation vulnerability exists in the /bin/login functionality of Peplink Smart Reader v1.2.0 (in QEMU). A specially crafted command line argument can lead to a limited-shell escape and elevated capabilities. An attacker can authenticate with hard-coded credentials and execute unblocked default busybox functionality to trigger this vulnerability. | 6.8 | More Details |
| CVE-2024-0671 | Use After Free vulnerability in Arm Ltd Midgard GPU Kernel Driver, Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory.This issue affects Midgard GPU Kernel Driver: from r19p0 through r32p0; Bifrost GPU Kernel Driver: from r7p0 through r48p0; Valhall GPU Kernel Driver: from r19p0 through r48p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r48p0. | 6.8 | More Details |
| CVE-2024-2761 | The Genesis Blocks WordPress plugin before 3.1.3 does not properly escape data input provided to some of its blocks, allowing using with at least contributor privileges to conduct Stored XSS attacks. | 6.8 | More Details |
| CVE-2024-32344 | A cross-site scripting (XSS) vulnerability in the Settings menu of CMSimple v5.15 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Edit parameter under the Language section. | 6.8 | More Details |
| CVE-2023-50885 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AGILELOGIX Store Locator WordPress.This issue affects Store Locator WordPress: from n/a through 1.4.14. | 6.8 | More Details |
| CVE-2024-31804 | An unquoted service path vulnerability in Terratec DMX_6Fire USB v.1.23.0.02 allows a local attacker to escalate privileges via the Program.exe component. | 6.7 | More Details |
| CVE-2024-32290 | Tenda W30E v1.0 v1.0.1.25(633) firmware has a stack overflow vulnerability via the page parameter in the fromAddressNat function. | 6.7 | More Details |
| CVE-2023-51797 | Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/avf_showwaves.c:722:24 in showwaves_filter_frame | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26828 | In the Linux kernel, the following vulnerability has been resolved: cifs: fix underflow in parse_server_interfaces() In this loop, we step through the buffer and after each item we check if the size_left is greater than the minimum size we need. However, the problem is that "bytes_left" is type ssize_t while sizeof() is type size_t. That means that because of type promotion, the comparison is done as an unsigned and if we have negative bytes left the loop continues instead of ending. | 6.7 | More Details |
| CVE-2024-30925 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows attackers to execute arbitrary code via the photo-thumbs.php component. | 6.5 | More Details |
| CVE-2024-32594 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AttesaWP Attesa Extra allows Stored XSS.This issue affects Attesa Extra: from n/a through 1.3.9. | 6.5 | More Details |
| CVE-2023-27279 | IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a user to cause a denial of service due to missing API rate limiting. IBM X-Force ID: 248533. | 6.5 | More Details |
| CVE-2024-31587 | SecuSTATION Camera V2.5.5.3116-S50-SMA-B20160811A and lower allows an unauthenticated attacker to download device configuration files via a crafted request. | 6.5 | More Details |
| CVE-2024-32593 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBits WPBITS Addons For Elementor Page Builder allows Stored XSS.This issue affects WPBITS Addons For Elementor Page Builder: from n/a through 1.3.4.2. | 6.5 | More Details |
| CVE-2024-32552 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tagbox Taggbox allows Stored XSS.This issue affects Taggbox: from n/a through 3.2. | 6.5 | More Details |
| CVE-2024-32592 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VoidCoders, innovs Void Elementor WHMCS Elements For Elementor Page Builder allows Stored XSS.This issue affects Void Elementor WHMCS Elements For Elementor Page Builder: from n/a through 2.0. | 6.5 | More Details |
| CVE-2024-32590 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webfood Kattene allows Stored XSS.This issue affects Kattene: from n/a through 1.7. | 6.5 | More Details |
| CVE-2024-3911 | An unauthenticated remote attacker can deceive users into performing unintended actions due to improper restriction of rendered UI layers or frames. | 6.5 | More Details |
| CVE-2023-49275 | Wazuh is a free and open source platform used for threat prevention, detection, and response. A NULL pointer dereference was detected during fuzzing of the analysis engine, allowing malicious clients to DoS the analysis engine. The bug occurs when `analysisd` receives a syscollector message with the `hotfix` `msg_type` but lacking a `timestamp`. It uses `cJSON_GetObjectItem()` to get the `timestamp` object item and dereferences it without checking for a `NULL` value. A malicious client can DoS the analysis engine. This vulnerability is fixed in 4.7.1. | 6.5 | More Details |
| CVE-2024-32334 | TOTOLINK N300RT V2.1.8-B20201030.1539 contains a Store Cross-site scripting (XSS) vulnerability in IP/Port Filtering under the Firewall Page. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-31208 | Synapse is an open-source Matrix homeserver. A remote Matrix user with malicious intent, sharing a room with Synapse instances before 1.105.1, can dispatch specially crafted events to exploit a weakness in the V2 state resolution algorithm. This can induce high CPU consumption and accumulate excessive data in the database of such instances, resulting in a denial of service. Servers in private federations, or those that do not federate, are not affected. Server administrators should upgrade to 1.105.1 or later. Some workarounds are available. One can ban the malicious users or ACL block servers from the rooms and/or leave the room and purge the room using the admin API. | 6.5 | More Details |
| CVE-2023-49768 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FormAssembly / Drew Buschhorn WP-FormAssembly allows Stored XSS.This issue affects WP-FormAssembly: from n/a through 2.0.10. | 6.5 | More Details |
| CVE-2024-33213 | Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the mitInterface parameter in ip/goform/RouteStatic. | 6.5 | More Details |
| CVE-2024-2798 | The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget containers in all versions up to, and including, 1.3.971 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. | 6.5 | More Details |
| CVE-2024-32470 | Tolgee is an open-source localization platform. When API key created by admin user is used it bypasses the permission check at all. This error was introduced in v3.57.2 and immediately fixed in v3.57.4. | 6.5 | More Details |
| CVE-2024-29956 | A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a prints the Brocade SANnav password in clear text in supportsave logs when a user schedules a switch Supportsave from Brocade SANnav. | 6.5 | More Details |
| CVE-2024-29987 | Microsoft Edge (Chromium-based) Information Disclosure Vulnerability | 6.5 | More Details |
| CVE-2023-3675 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Secomea GateManager (Web GUI) allows Reading Data from System Resources.This issue affects GateManager: from 11.0.623074018 before 11.0.623373051. | 6.5 | More Details |
| CVE-2024-32596 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric-Oliver Mächler DSGVO Youtube allows Stored XSS.This issue affects DSGVO Youtube: from n/a through 1.4.5. | 6.5 | More Details |
| CVE-2024-32569 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metaphor Creations Ditty allows Stored XSS.This issue affects Ditty: from n/a through 3.1.31. | 6.5 | More Details |
| CVE-2024-32571 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in naa986 WP Stripe Checkout allows Stored XSS.This issue affects WP Stripe Checkout: from n/a through 1.2.2.41. | 6.5 | More Details |
| CVE-2024-32572 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 5.6.0. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32566 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Club Manager allows Stored XSS.This issue affects WP Club Manager: from n/a through 2.2.11. | 6.5 | More Details |
| CVE-2024-32565 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Appcheap.Io App Builder allows Stored XSS.This issue affects App Builder: from n/a through 3.8.8. | 6.5 | More Details |
| CVE-2024-22807 | An issue in Tormach xsTECH CNC Router, PathPilot Controller v2.9.6 allows attackers to erase a critical sector of the flash memory, causing the machine to lose network connectivity and suffer from firmware corruption. | 6.5 | More Details |
| CVE-2024-32575 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kraftplugins Mega Elements allows Stored XSS.This issue affects Mega Elements: from n/a through 1.1.9. | 6.5 | More Details |
| CVE-2024-32561 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tagembed allows Stored XSS.This issue affects Tagembed: from n/a through 4.7. | 6.5 | More Details |
| CVE-2024-32688 | Missing Authorization vulnerability in Long Watch Studio MyRewards.This issue affects MyRewards: from n/a through 5.3.0. | 6.5 | More Details |
| CVE-2024-32576 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Booking Algorithms BA Book Everything allows Stored XSS.This issue affects BA Book Everything: from n/a through 1.6.8. | 6.5 | More Details |
| CVE-2024-32560 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sharabindu QR Code Composer allows Stored XSS.This issue affects QR Code Composer: from n/a through 2.0.3. | 6.5 | More Details |
| CVE-2024-32577 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codeboxr Team CBX Bookmark & Favorite cbxwpbookmark allows Stored XSS.This issue affects CBX Bookmark & Favorite: from n/a through 1.7.20. | 6.5 | More Details |
| CVE-2024-32579 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GloriaFood Restaurant Menu – Food Ordering System – Table Reservation allows Stored XSS.This issue affects Restaurant Menu – Food Ordering System – Table Reservation: from n/a through 2.4.1. | 6.5 | More Details |
| CVE-2024-32580 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Averta Master Slider allows Stored XSS.This issue affects Master Slider: from n/a through 3.9.8. | 6.5 | More Details |
| CVE-2024-32698 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leevio Happy Addons for Elementor allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.10.4. | 6.5 | More Details |
| CVE-2024-32697 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HelloAsso allows Stored XSS.This issue affects HelloAsso: from n/a through 1.1.5. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32696 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuantumCloud Infographic Maker – iList allows Stored XSS.This issue affects Infographic Maker – iList: from n/a through 4.6.6. | 6.5 | More Details |
| CVE-2024-32556 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nabil Lemsieh HurryTimer allows Stored XSS.This issue affects HurryTimer: from n/a through 2.9.2. | 6.5 | More Details |
| CVE-2024-32581 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lenderd Mortgage Calculators WP allows Stored XSS.This issue affects Mortgage Calculators WP: from n/a through 1.56. | 6.5 | More Details |
| CVE-2024-31994 | Mealie is a self hosted recipe manager and meal planner. Prior to 1.4.0, an attacker can point the image request to an arbitrarily large file. Mealie will attempt to retrieve this file in whole. If it can be retrieved, it may be stored on the file system in whole (leading to possible disk consumption), however the more likely scenario given resource limitations is that the container will OOM during file retrieval if the target file size is greater than the allocated memory of the container. At best this can be used to force the container to infinitely restart due to OOM (if so configured in `docker-compose.yml), or at worst this can be used to force the Mealie container to crash and remain offline. In the event that the file can be retrieved, the lack of rate limiting on this endpoint also permits an attacker to generate ongoing requests to any target of their choice, potentially contributing to an external-facing DoS attack. This vulnerability is fixed in 1.4.0. | 6.5 | More Details |
| CVE-2024-29368 | An arbitrary file upload vulnerability in the file handling module of moziloCMS v2.0 allows attackers to bypass extension restrictions via file renaming, potentially leading to unauthorized file execution or storage of malicious content. | 6.5 | More Details |
| CVE-2024-31992 | Mealie is a self hosted recipe manager and meal planner. Prior to 1.4.0, the safe_scrape_html function utilizes a user-controlled URL to issue a request to a remote server, however these requests are not rate-limited. While there are efforts to prevent DDoS by implementing a timeout on requests, it is possible for an attacker to issue a large number of requests to the server which will be handled in batches based on the configuration of the Mealie server. The chunking of responses is helpful for mitigating memory exhaustion on the Mealie server, however a single request to an arbitrarily large external file (e.g. a Debian ISO) is often sufficient to completely saturate a CPU core assigned to the Mealie container. Without rate limiting in place, it is possible to not only sustain traffic against an external target indefinitely, but also to exhaust the CPU resources assigned to the Mealie container. This vulnerability is fixed in 1.4.0. | 6.5 | More Details |
| CVE-2024-32554 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Knight Lab Knight Lab Timeline allows Stored XSS.This issue affects Knight Lab Timeline: from n/a through 3.9.3.4. | 6.5 | More Details |
| CVE-2024-32586 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Munir Kamal Gutenberg Block Editor Toolkit allows Stored XSS.This issue affects Gutenberg Block Editor Toolkit: from n/a through 1.40.4. | 6.5 | More Details |
| CVE-2024-22809 | Incorrect access control in Tormach xsTECH CNC Router, PathPilot Controller v2.9.6 allows attackers to access the G code's shared folder and view sensitive information. | 6.5 | More Details |
| CVE-2024-32564 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Post Grid Team by WPXPO PostX – Gutenberg Blocks for Post Grid allows Stored XSS.This issue affects PostX – Gutenberg Blocks for Post Grid: from n/a through 4.0.1. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32536 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Trade Pips WP TradingView allows Stored XSS.This issue affects WP TradingView: from n/a through 1.7. | 6.5 | More Details |
| CVE-2024-32508 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in deTheme DethemeKit For Elementor allows Stored XSS.This issue affects DethemeKit For Elementor: from n/a through 2.0.2. | 6.5 | More Details |
| CVE-2024-3914 | Use after free in V8 in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) | 6.5 | More Details |
| CVE-2024-32316 | Tenda AC500 V2.0.1.9(1307) firmware has a stack overflow vulnerability in the fromDhcpListClient function. | 6.5 | More Details |
| CVE-2024-30986 | Cross Site Scripting vulnerability in /edit-services-details.php of phpgurukul Client Management System using PHP & MySQL 1.1 allows attackers to execute arbitrary code and via "price" and "sname" parameter. | 6.5 | More Details |
| CVE-2024-32313 | Tenda FH1205 V2.0.0.7(775) firmware has a stack overflow vulnerability located via the adslPwd parameter of the formWanParameterSetting function. | 6.5 | More Details |
| CVE-2024-32287 | Tenda W30E v1.0 V1.0.1.25(633) firmware has a stack overflow vulnerability via the qos parameter in the fromqossetting function. | 6.5 | More Details |
| CVE-2024-32509 | Missing Authorization vulnerability in Loopus WP Cost Estimation & Payment Forms Builder.This issue affects WP Cost Estimation & Payment Forms Builder: from n/a through 10.1.76. | 6.5 | More Details |
| CVE-2024-32130 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paystack Payment Forms for Paystack allows Stored XSS.This issue affects Payment Forms for Paystack: from n/a through 3.4.1. | 6.5 | More Details |
| CVE-2024-3839 | Out of bounds read in Fonts in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium) | 6.5 | More Details |
| CVE-2024-32456 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EnvoThemes Envo Extra allows Stored XSS.This issue affects Envo Extra: from n/a through 1.8.11. | 6.5 | More Details |
| CVE-2024-32505 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpmet Elements kit Elementor addons allows Stored XSS.This issue affects Elements kit Elementor addons: from n/a through 3.0.6. | 6.5 | More Details |
| CVE-2024-32457 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The CSSIgniter Team Elements Plus! allows Stored XSS.This issue affects Elements Plus!: from n/a through 2.16.3. | 6.5 | More Details |
| CVE-2024-32526 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Flector Easy Textillate allows Stored XSS.This issue affects Easy Textillate: from n/a through 2.02. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26890 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btrtl: fix out of bounds memory access The problem is detected by KASAN. btrtl driver uses private hci data to store 'struct btrealtek_data'. If btrtl driver is used with btusb, then memory for private hci data is allocated in btusb. But no private data is allocated after hci_dev, when btrtl is used with hci_h5. This commit adds memory allocation for hci_h5 case. ================================================================== BUG: KASAN: slab-out-of-bounds in btrtl_initialize+0x6cc/0x958 [btrtl] Write of size 8 at addr ffff00000f5a5748 by task kworker/u9:0/76 Hardware name: Pine64 PinePhone (1.2) (DT) Workqueue: hci0 hci_power_on [bluetooth] Call trace: dump_backtrace+0x9c/0x128 show_stack+0x20/0x38 dump_stack_lvl+0x48/0x60 print_report+0xf8/0x5d8 kasan_report+0x90/0xd0 __asan_store8+0x9c/0xc0 [btrtl] h5_btrtl_setup+0xd0/0x2f8 [hci_uart] h5_setup+0x50/0x80 [hci_uart] hci_uart_setup+0xd4/0x260 [hci_uart] hci_dev_open_sync+0x1cc/0xf68 [bluetooth] hci_dev_do_open+0x34/0x90 [bluetooth] hci_power_on+0xc4/0x3c8 [bluetooth] process_one_work+0x328/0x6f0 worker_thread+0x410/0x778 kthread+0x168/0x178 ret_from_fork+0x10/0x20 Allocated by task 53: kasan_save_stack+0x3c/0x68 kasan_save_track+0x20/0x40 kasan_save_alloc_info+0x68/0x78 __kasan_kmalloc+0xd4/0xd8 __kmalloc+0x1b4/0x3b0 hci_alloc_dev_priv+0x28/0xa58 [bluetooth] hci_uart_register_device+0x118/0x4f8 [hci_uart] h5_serdev_probe+0xf4/0x178 [hci_uart] serdev_drv_probe+0x54/0xa0 really_probe+0x254/0x588 __driver_probe_device+0xc4/0x210 driver_probe_device+0x64/0x160 __driver_attach_async_helper+0x88/0x158 async_run_entry_fn+0xd0/0x388 process_one_work+0x328/0x6f0 worker_thread+0x410/0x778 kthread+0x168/0x178 ret_from_fork+0x10/0x20 Last potentially related work creation: kasan_save_stack+0x3c/0x68 __kasan_record_aux_stack+0xb0/0x150 kasan_record_aux_stack_noalloc+0x14/0x20 __queue_work+0x33c/0x960 queue_work_on+0x98/0xc0 hci_recv_frame+0xc8/0x1e8 [bluetooth] h5_complete_rx_pkt+0x2c8/0x800 [hci_uart] h5_rx_payload+0x98/0xb8 [hci_uart] h5_recv+0x158/0x3d8 [hci_uart] hci_uart_receive_buf+0xa0/0xe8 [hci_uart] ttyport_receive_buf+0xac/0x178 flush_to_ldisc+0x130/0x2c8 process_one_work+0x328/0x6f0 worker_thread+0x410/0x778 kthread+0x168/0x178 ret_from_fork+0x10/0x20 Second to last potentially related work creation: kasan_save_stack+0x3c/0x68 __kasan_record_aux_stack+0xb0/0x150 kasan_record_aux_stack_noalloc+0x14/0x20 __queue_work+0x788/0x960 queue_work_on+0x98/0xc0 __hci_cmd_sync_sk+0x23c/0x7a0 [bluetooth] __hci_cmd_sync+0x24/0x38 [bluetooth] btrtl_initialize+0x760/0x958 [btrtl] h5_btrtl_setup+0xd0/0x2f8 [hci_uart] h5_setup+0x50/0x80 [hci_uart] hci_uart_setup+0xd4/0x260 [hci_uart] hci_dev_open_sync+0x1cc/0xf68 [bluetooth] hci_dev_do_open+0x34/0x90 [bluetooth] hci_power_on+0xc4/0x3c8 [bluetooth] process_one_work+0x328/0x6f0 worker_thread+0x410/0x778 kthread+0x168/0x178 ret_from_fork+0x10/0x20 ================================================================== | 6.5 | More Details |
| CVE-2024-32539 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JoomUnited WP File Download Light allows Stored XSS.This issue affects WP File Download Light: from n/a through 1.3.3. | 6.5 | More Details |
| CVE-2024-32311 | Tenda FH1203 v2.0.1.6 firmware has a stack overflow vulnerability via the adslPwd parameter in the formWanParameterSetting function. | 6.5 | More Details |
| CVE-2024-32527 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jotform Jotform Online Forms allows Stored XSS.This issue affects Jotform Online Forms: from n/a through 1.3.1. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26886 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: af_bluetooth: Fix deadlock Attemting to do sock_lock on .recvmsg may cause a deadlock as shown bellow, so instead of using sock_sock this uses sk_receive_queue.lock on bt_sock_ioctl to avoid the UAF: INFO: task kworker/u9:1:121 blocked for more than 30 seconds. Not tainted 6.7.6-lemon #183 Workqueue: hci0 hci_rx_work Call Trace: <TASK> __schedule+0x37d/0xa00 schedule+0x32/0xe0 __lock_sock+0x68/0xa0 ? __pfx_autoremove_wake_function+0x10/0x10 lock_sock_nested+0x43/0x50 l2cap_sock_recv_cb+0x21/0xa0 l2cap_recv_frame+0x55b/0x30a0 ? psi_task_switch+0xeb/0x270 ? finish_task_switch.isra.0+0x93/0x2a0 hci_rx_work+0x33a/0x3f0 process_one_work+0x13a/0x2f0 worker_thread+0x2f0/0x410 ? __pfx_worker_thread+0x10/0x10 kthread+0xe0/0x110 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2c/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> | 6.5 | More Details |
| CVE-2022-41698 | Missing Authorization vulnerability in Layered If Menu.This issue affects If Menu: from n/a through 0.16.3. | 6.5 | More Details |
| CVE-2024-32530 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PressTigers Simple Testimonials Showcase allows Stored XSS.This issue affects Simple Testimonials Showcase: from n/a through 1.1.5. | 6.5 | More Details |
| CVE-2024-32529 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Momoyoga Yoga Schedule Momoyoga allows Stored XSS.This issue affects Yoga Schedule Momoyoga: from n/a through 2.7.0. | 6.5 | More Details |
| CVE-2024-3560 | The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _id value in all versions up to, and including, 4.2.6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2023-6805 | The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 4.4.7 via the fetch_feed functionality. This makes it possible for authenticated attackers, with contributor access and above, to make web requests to arbitrary locations originating from the web application and can be used to modify information from internal services. NOTE: This vulnerability, exploitable by contributor-level users, was was fixed in version 4.4.7. The same vulnerability was fixed for author-level users in version 4.4.8. | 6.4 | More Details |
| CVE-2024-3645 | The Essential Addons for Elementor Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Counter widget in all versions up to, and including, 5.8.11 due to insufficient input sanitization and output escaping on user supplied attributes such as 'title_html_tag'. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2024-29376 | Sylius 1.12.13 is vulnerable to Cross Site Scripting (XSS) via the "Province" field in Address Book. | 6.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3889 | The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Advanced Accordion widget in all versions up to, and including, 1.3.971 due to insufficient input sanitization and output escaping on user supplied attributes like 'accordion_title_tag'. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2023-6892 | The EAN for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'alg_wc_ean_product_meta' shortcode in all versions up to, and including, 4.8.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2024-3333 | The Essential Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL attributes of widgets in all versions up to, and including, 5.9.14 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-2024-2799 | The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Grid & Advanced Text widget HTML tags in all versions up to, and including, 1.3.96 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-2024-3598 | The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Creative Button widget in all versions up to, and including, 3.6.0 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-2024-2477 | The wpDiscuz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Alternative Text' field of an uploaded image in all versions up to, and including, 7.6.15 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-2024-1426 | The Element Pack Elementor Addons (Header Footer, Free Template Library, Grid, Carousel, Table, Parallax Animation, Register Form, Twitter Grid) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘link’ attribute of the Price List widget in all versions up to, and including, 5.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26875 | In the Linux kernel, the following vulnerability has been resolved: media: pvrusb2: fix uaf in pvr2_context_set_notify [Syzbot reported] BUG: KASAN: slab-use-after-free in pvr2_context_set_notify+0x2c4/0x310 drivers/media/usb/pvrusb2/pvrusb2-context.c:35 Read of size 4 at addr ffff888113aeb0d8 by task kworker/1:1/26 CPU: 1 PID: 26 Comm: kworker/1:1 Not tainted 6.8.0-rc1-syzkaller-00046-gf1a27f081c1f #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/25/2024 Workqueue: usb_hub_wq hub_event Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x1b0 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc4/0x620 mm/kasan/report.c:488 kasan_report+0xda/0x110 mm/kasan/report.c:601 pvr2_context_set_notify+0x2c4/0x310 drivers/media/usb/pvrusb2/pvrusb2-context.c:35 pvr2_context_notify drivers/media/usb/pvrusb2/pvrusb2-context.c:95 [inline] pvr2_context_disconnect+0x94/0xb0 drivers/media/usb/pvrusb2/pvrusb2-context.c:272 Freed by task 906: kasan_save_stack+0x33/0x50 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 kasan_save_free_info+0x3f/0x60 mm/kasan/generic.c:640 poison_slab_object mm/kasan/common.c:241 [inline] __kasan_slab_free+0x106/0x1b0 mm/kasan/common.c:257 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2121 [inline] slab_free mm/slub.c:4299 [inline] kfree+0x105/0x340 mm/slub.c:4409 pvr2_context_check drivers/media/usb/pvrusb2/pvrusb2-context.c:137 [inline] pvr2_context_thread_func+0x69d/0x960 drivers/media/usb/pvrusb2/pvrusb2-context.c:158 [Analyze] Task A set disconnect_flag = !0, which resulted in Task B's condition being met and releasing mp, leading to this issue. [Fix] Place the disconnect_flag assignment operation after all code in pvr2_context_disconnect() to avoid this issue. | 6.4 | More Details |
| CVE-2024-32163 | CMSeasy 7.7.7.9 is vulnerable to code execution. | 6.4 | More Details |
| CVE-2024-1057 | The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +10 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wishsuite_button' shortcode in all versions up to, and including, 2.8.1 due to insufficient input sanitization and output escaping on user supplied attributes like 'button_class'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2024-3665 | The Rank Math SEO with AI SEO Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's HowTo and FAQ widgets in all versions up to, and including, 1.0.216 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-2024-4014 | The hCaptcha for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cf7-hcaptcha shortcode in all versions up to, and including, 4.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-1429 | The Element Pack Elementor Addons (Header Footer, Free Template Library, Grid, Carousel, Table, Parallax Animation, Register Form, Twitter Grid) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘tab_link’ attribute of the Panel Slider widget in all versions up to, and including, 5.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 6.4 | More Details |
| CVE-2024-3491 | The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's "How To" and "FAQ" Blocks in all versions up to, and including, 1.29 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-2024-3732 | The GeoDirectory – WordPress Business Directory Plugin, or Classified Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gd_single_tabs' shortcode in all versions up to, and including, 2.3.48 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-2024-3948 | A vulnerability was found in SourceCodester Home Clean Service System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file \admin\student.add.php of the component Photo Handler. The manipulation leads to unrestricted upload. 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-261440. | 6.3 | More Details |
| CVE-2024-4019 | A vulnerability classified as critical has been found in Byzoro Smart S80 Management Platform up to 20240411. Affected is an unknown function of the file /importhtml.php. The manipulation of the argument sql leads to deserialization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-261666 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 6.3 | More Details |
| CVE-2024-32282 | Tenda FH1202 v1.2.0.14(408) firmware contains a command injection vulnerablility in the formexeCommand function via the cmdinput parameter. | 6.3 | More Details |
| CVE-2024-32288 | Tenda W30E v1.0 V1.0.1.25(633) firmware has a stack overflow vulnerability located via the page parameter in the fromwebExcptypemanFilter function. | 6.3 | More Details |
| CVE-2024-3908 | A vulnerability classified as critical has been found in Tenda AC500 2.0.1.9(1307). Affected is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-261144. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 6.3 | More Details |
| CVE-2024-30927 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows attackers to execute arbitrary code via the racer-results.php component. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26880 | In the Linux kernel, the following vulnerability has been resolved: dm: call the resume method on internal suspend There is this reported crash when experimenting with the lvm2 testsuite. The list corruption is caused by the fact that the postsuspend and resume methods were not paired correctly; there were two consecutive calls to the origin_postsuspend function. The second call attempts to remove the "hash_list" entry from a list, while it was already removed by the first call. Fix __dm_internal_resume so that it calls the preresume and resume methods of the table's targets. If a preresume method of some target fails, we are in a tricky situation. We can't return an error because dm_internal_resume isn't supposed to return errors. We can't return success, because then the "resume" and "postsuspend" methods would not be paired correctly. So, we set the DMF_SUSPENDED flag and we fake normal suspend - it may confuse userspace tools, but it won't cause a kernel crash. ------------[ cut here ]------------ kernel BUG at lib/list_debug.c:56! invalid opcode: 0000 [#1] PREEMPT SMP CPU: 1 PID: 8343 Comm: dmsetup Not tainted 6.8.0-rc6 #4 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-2 04/01/2014 RIP: 0010:__list_del_entry_valid_or_report+0x77/0xc0 <snip> RSP: 0018:ffff8881b831bcc0 EFLAGS: 00010282 RAX: 000000000000004e RBX: ffff888143b6eb80 RCX: 0000000000000000 RDX: 0000000000000001 RSI: ffffffff819053d0 RDI: 00000000ffffffff RBP: ffff8881b83a3400 R08: 00000000fffeffff R09: 0000000000000058 R10: 0000000000000000 R11: ffffffff81a24080 R12: 0000000000000001 R13: ffff88814538e000 R14: ffff888143bc6dc0 R15: ffffffffa02e4bb0 FS: 00000000f7c0f780(0000) GS:ffff8893f0a40000(0000) knlGS:0000000000000000 CS: 0010 DS: 002b ES: 002b CR0: 0000000080050033 CR2: 0000000057fb5000 CR3: 0000000143474000 CR4: 00000000000006b0 Call Trace: <TASK> ? die+0x2d/0x80 ? do_trap+0xeb/0xf0 ? __list_del_entry_valid_or_report+0x77/0xc0 ? do_error_trap+0x60/0x80 ? __list_del_entry_valid_or_report+0x77/0xc0 ? exc_invalid_op+0x49/0x60 ? __list_del_entry_valid_or_report+0x77/0xc0 ? asm_exc_invalid_op+0x16/0x20 ? table_deps+0x1b0/0x1b0 [dm_mod] ? __list_del_entry_valid_or_report+0x77/0xc0 origin_postsuspend+0x1a/0x50 [dm_snapshot] dm_table_postsuspend_targets+0x34/0x50 [dm_mod] dm_suspend+0xd8/0xf0 [dm_mod] dev_suspend+0x1f2/0x2f0 [dm_mod] ? table_deps+0x1b0/0x1b0 [dm_mod] ctl_ioctl+0x300/0x5f0 [dm_mod] dm_compat_ctl_ioctl+0x7/0x10 [dm_mod] __x64_compat_sys_ioctl+0x104/0x170 do_syscall_64+0x184/0x1b0 entry_SYSCALL_64_after_hwframe+0x46/0x4e RIP: 0033:0xf7e6aead <snip> ---[ end trace 0000000000000000 ]--- | 6.3 | More Details |
| CVE-2024-3654 | An XSS vulnerability has been found in Teimas Global's Teixo, version 1.42.42-stable. This vulnerability could allow an attacker to send a specially crafted JavaScript payload via the "seconds" parameter in the program's URL, resulting in a possible takeover of a registered user's session. | 6.3 | More Details |
| CVE-2024-28722 | Cross Site Scripting vulnerability in Innovaphone myPBX v.14r1, v.13r3, v.12r2 allows a remote attacker to execute arbitrary code via the query parameter to the /CMD0/xml_modes.xml endpoint | 6.3 | More Details |
| CVE-2024-32302 | Tenda FH1202 v1.2.0.14(408) firmware has a stack overflow vulnerability via the PPW parameter in the fromWizardHandle function. | 6.3 | More Details |
| CVE-2024-4071 | A vulnerability was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0 and classified as critical. This issue affects some unknown processing of the file prodInfo.php. The manipulation of the argument prodId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261797 was assigned to this vulnerability. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-4070 | A vulnerability has been found in Kashipara Online Furniture Shopping Ecommerce Website 1.0 and classified as critical. This vulnerability affects unknown code of the file prodList.php. The manipulation of the argument prodType leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-261796. | 6.3 | More Details |
| CVE-2024-4069 | A vulnerability, which was classified as critical, was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0. This affects an unknown part of the file search.php. The manipulation of the argument txtSearch leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-261795. | 6.3 | More Details |
| CVE-2024-26918 | In the Linux kernel, the following vulnerability has been resolved: PCI: Fix active state requirement in PME polling The commit noted in fixes added a bogus requirement that runtime PM managed devices need to be in the RPM_ACTIVE state for PME polling. In fact, only devices in low power states should be polled. However there's still a requirement that the device config space must be accessible, which has implications for both the current state of the polled device and the parent bridge, when present. It's not sufficient to assume the bridge remains in D0 and cases have been observed where the bridge passes the D0 test, but the PM state indicates RPM_SUSPENDING and config space of the polled device becomes inaccessible during pci_pme_wakeup(). Therefore, since the bridge is already effectively required to be in the RPM_ACTIVE state, formalize this in the code and elevate the PM usage count to maintain the state while polling the subordinate device. This resolves a regression reported in the bugzilla below where a Thunderbolt/USB4 hierarchy fails to scan for an attached NVMe endpoint downstream of a bridge in a D3hot power state. | 6.2 | More Details |
| CVE-2023-38300 | A certain software build for the Orbic Maui device (Orbic/RC545L/RC545L:10/ORB545L_V1.4.2_BVZPP/230106:user/release-keys) leaks the IMEI and the ICCID to system properties that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in this instance they are leaked by a high-privilege process and can be obtained indirectly. This malicious app reads from the "persist.sys.verizon_test_plan_imei" system property to indirectly obtain the IMEI and reads the "persist.sys.verizon_test_plan_iccid" system property to obtain the ICCID. | 6.2 | More Details |
| CVE-2024-31993 | Mealie is a self hosted recipe manager and meal planner. Prior to 1.4.0, the scrape_image function will retrieve an image based on a user-provided URL, however the provided URL is not validated to point to an external location and does not have any enforced rate limiting. The response from the Mealie server will also vary depending on whether or not the target file is an image, is not an image, or does not exist. Additionally, when a file is retrieved the file may remain stored on Mealie’s file system as original.jpg under the UUID of the recipe it was requested for. If the attacker has access to an admin account (e.g. the default changeme@example.com), this file can then be retrieved. Note that if Mealie is running in a development setting this could be leveraged by an attacker to retrieve any file that the Mealie server had downloaded in this fashion without the need for administrator access. This vulnerability is fixed in 1.4.0. | 6.2 | More Details |
| CVE-2024-30951 | FUDforum v3.1.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the chpos parameter at /adm/admsmiley.php. | 6.1 | More Details |
| CVE-2024-32332 | TOTOLINK N300RT V2.1.8-B20201030.1539 contains a Store Cross-site scripting (XSS) vulnerability in WDS Settings under the Wireless Page. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-38294 | Certain software builds for the Itel Vision 3 Turbo Android device contain a vulnerable pre-installed app with a package name of com.transsion.autotest.factory (versionCode='7', versionName='1.8.0(220310_1027)') that allows local third-party apps to execute arbitrary shell commands in its context (system user) due to inadequate access control. No permissions or special privileges are necessary to exploit the vulnerability in the com.transsion.autotest.factory app. No user interaction is required beyond installing and running a third-party app. The vulnerability allows local apps to access sensitive functionality that is generally restricted to pre-installed apps, such as programmatically performing the following actions: granting arbitrary permissions (which can be used to obtain sensitive user data), installing arbitrary apps, video recording the screen, wiping the device (removing the user's apps and data), injecting arbitrary input events, calling emergency phone numbers, disabling apps, accessing notifications, and much more. The confirmed vulnerable software build fingerprints for the Itel Vision 3 Turbo device are as follows: Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V92-20230105:user/release-keys, Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V86-20221118:user/release-keys, Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V78-20221101:user/release-keys, Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V64-20220803:user/release-keys, Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V61-20220721:user/release-keys, Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V58-20220712:user/release-keys, and Itel/F6321/itel-S661LP:11/RP1A.201005.001/GL-V051-20220613:user/release-keys. This malicious app sends a broadcast Intent to the receiver component named com.transsion.autotest.factory/.broadcast.CommandReceiver with the path to a shell script that it creates in its scoped storage directory. Then the com.transsion.autotest.factory app will execute the shell script with "system" privileges. | 6.1 | More Details |
| CVE-2022-34562 | A cross-site scripting (XSS) vulnerability in PHPFox v4.8.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the status box. | 6.1 | More Details |
| CVE-2024-32875 | Hugo is a static site generator. Starting in version 0.123.0 and prior to version 0.125.3, title arguments in Markdown for links and images not escaped in internal render hooks. Hugo users who are impacted are those who have these hooks enabled and do not trust their Markdown content files. The issue is patched in v0.125.3. As a workaround, replace the templates with user defined templates or disable the internal templates. | 6.1 | More Details |
| CVE-2024-32472 | excalidraw is an open source virtual hand-drawn style whiteboard. A stored XSS vulnerability in Excalidraw's web embeddable component. This allows arbitrary JavaScript to be run in the context of the domain where the editor is hosted. There were two vectors. One rendering untrusted string as iframe's `srcdoc` without properly sanitizing against HTML injection. Second by improperly sanitizing against attribute HTML injection. This in conjunction with allowing `allow-same-origin` sandbox flag (necessary for several embeds) resulted in the XSS. This vulnerability is fixed in 0.17.6 and 0.16.4. | 6.1 | More Details |
| CVE-2024-27306 | aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. A XSS vulnerability exists on index pages for static file handling. This vulnerability is fixed in 3.9.4. We have always recommended using a reverse proxy server (e.g. nginx) for serving static files. Users following the recommendation are unaffected. Other users can disable `show_index` if unable to upgrade. | 6.1 | More Details |
| CVE-2024-2729 | The Otter Blocks WordPress plugin before 2.6.6 does not properly escape its mainHeadings blocks' attribute before appending it to the final rendered block, allowing contributors to conduct Stored XSS attacks. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-29183 | OpenRASP is a RASP solution that directly integrates its protection engine into the application server by instrumentation. There exists a reflected XSS in the /login page due to a reflection of the redirect parameter. This allows an attacker to execute arbitrary javascript with the permissions of a user after the user logins with their account. | 6.1 | More Details |
| CVE-2024-29029 | memos is a privacy-first, lightweight note-taking service. In memos 0.13.2, an SSRF vulnerability exists at the /o/get/image that allows unauthenticated users to enumerate the internal network and retrieve images. The response from the image request is then copied into the response of the current server request, causing a reflected XSS vulnerability. Version 0.22.0 of memos removes the vulnerable file. | 6.1 | More Details |
| CVE-2024-32339 | Multiple cross-site scripting (XSS) vulnerabilities in the HOW TO page of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into any of the parameters. | 6.1 | More Details |
| CVE-2024-30953 | A stored cross-site scripting (XSS) vulnerability in Htmly v2.9.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Link Name parameter of Menu Editor module. | 6.1 | More Details |
| CVE-2024-32342 | A cross-site scripting (XSS) vulnerability in the Create Page of Boid CMS v2.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Permalink parameter. | 6.1 | More Details |
| CVE-2024-3731 | The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in all versions up to, and including, 5.47.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. | 6.1 | More Details |
| CVE-2024-32337 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the ADMIN LOGIN URL parameter under the Security module. | 6.1 | More Details |
| CVE-2024-2833 | The Jobs for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘job-search’ parameter in all versions up to, and including, 2.7.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. | 6.1 | More Details |
| CVE-2024-3841 | Insufficient data validation in Browser Switcher in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to inject scripts or HTML into a privileged page via a malicious file. (Chromium security severity: Medium) | 6.1 | More Details |
| CVE-2024-32343 | A cross-site scripting (XSS) vulnerability in the Create Page of Boid CMS v2.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Content parameter. | 6.1 | More Details |
| CVE-2024-3615 | The Media Library Folders plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in all versions up to, and including, 8.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32653 | jadx is a Dex to Java decompiler. Prior to version 1.5.0, the package name is not filtered before concatenation. This can be exploited to inject arbitrary code into the package name. The vulnerability allows an attacker to execute commands with shell privileges. Version 1.5.0 contains a patch for the vulnerability. | 6.1 | More Details |
| CVE-2024-28436 | Cross Site Scripting vulnerability in D-Link DAP products DAP-2230, DAP-2310, DAP-2330, DAP-2360, DAP-2553, DAP-2590, DAP-2690, DAP-2695, DAP-3520, DAP-3662 allows a remote attacker to execute arbitrary code via the reload parameter in the session_login.php component. | 6.1 | More Details |
| CVE-2024-3847 | Insufficient policy enforcement in WebUI in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low) | 6.1 | More Details |
| CVE-2024-26843 | In the Linux kernel, the following vulnerability has been resolved: efi: runtime: Fix potential overflow of soft-reserved region size md_size will have been narrowed if we have >= 4GB worth of pages in a soft-reserved region. | 6.0 | More Details |
| CVE-2024-26894 | In the Linux kernel, the following vulnerability has been resolved: ACPI: processor_idle: Fix memory leak in acpi_processor_power_exit() After unregistering the CPU idle device, the memory associated with it is not freed, leading to a memory leak: unreferenced object 0xffff896282f6c000 (size 1024): comm "swapper/0", pid 1, jiffies 4294893170 hex dump (first 32 bytes): 00 00 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc 8836a742): [<ffffffff993495ed>] kmalloc_trace+0x29d/0x340 [<ffffffff9972f3b3>] acpi_processor_power_init+0xf3/0x1c0 [<ffffffff9972d263>] __acpi_processor_start+0xd3/0xf0 [<ffffffff9972d2bc>] acpi_processor_start+0x2c/0x50 [<ffffffff99805872>] really_probe+0xe2/0x480 [<ffffffff99805c98>] __driver_probe_device+0x78/0x160 [<ffffffff99805daf>] driver_probe_device+0x1f/0x90 [<ffffffff9980601e>] __driver_attach+0xce/0x1c0 [<ffffffff99803170>] bus_for_each_dev+0x70/0xc0 [<ffffffff99804822>] bus_add_driver+0x112/0x210 [<ffffffff99807245>] driver_register+0x55/0x100 [<ffffffff9aee4acb>] acpi_processor_driver_init+0x3b/0xc0 [<ffffffff990012d1>] do_one_initcall+0x41/0x300 [<ffffffff9ae7c4b0>] kernel_init_freeable+0x320/0x470 [<ffffffff99b231f6>] kernel_init+0x16/0x1b0 [<ffffffff99042e6d>] ret_from_fork+0x2d/0x50 Fix this by freeing the CPU idle device after unregistering it. | 6.0 | More Details |
| CVE-2024-1065 | Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r45p0 through r48p0; Valhall GPU Kernel Driver: from r45p0 through r48p0; Arm 5th Gen GPU Architecture Kernel Driver: from r45p0 through r48p0. | 5.9 | More Details |
| CVE-2024-2118 | The Social Media Share Buttons & Social Sharing Icons WordPress plugin before 2.8.9 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) | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26864 | In the Linux kernel, the following vulnerability has been resolved: tcp: Fix refcnt handling in __inet_hash_connect(). syzbot reported a warning in sk_nulls_del_node_init_rcu(). The commit 66b60b0c8c4a ("dccp/tcp: Unhash sk from ehash for tb2 alloc failure after check_estalblished().") tried to fix an issue that an unconnected socket occupies an ehash entry when bhash2 allocation fails. In such a case, we need to revert changes done by check_established(), which does not hold refcnt when inserting socket into ehash. So, to revert the change, we need to __sk_nulls_add_node_rcu() instead of sk_nulls_add_node_rcu(). Otherwise, sock_put() will cause refcnt underflow and leak the socket. [0]: WARNING: CPU: 0 PID: 23948 at include/net/sock.h:799 sk_nulls_del_node_init_rcu+0x166/0x1a0 include/net/sock.h:799 Modules linked in: CPU: 0 PID: 23948 Comm: syz-executor.2 Not tainted 6.8.0-rc6-syzkaller-00159-gc055fc00c07b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/25/2024 RIP: 0010:sk_nulls_del_node_init_rcu+0x166/0x1a0 include/net/sock.h:799 Code: e8 7f 71 c6 f7 83 fb 02 7c 25 e8 35 6d c6 f7 4d 85 f6 0f 95 c0 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc e8 1b 6d c6 f7 90 <0f> 0b 90 eb b2 e8 10 6d c6 f7 4c 89 e7 be 04 00 00 00 e8 63 e7 d2 RSP: 0018:ffffc900032d7848 EFLAGS: 00010246 RAX: ffffffff89cd0035 RBX: 0000000000000001 RCX: 0000000000040000 RDX: ffffc90004de1000 RSI: 000000000003ffff RDI: 0000000000040000 RBP: 1ffff1100439ac26 R08: ffffffff89ccffe3 R09: 1ffff1100439ac28 R10: dfffffc0000000000 R11: ffffed100439ac29 R12: ffff888021cd6140 R13: dfffffc0000000000 R14: ffff88802a9bf5c0 R15: ffff888021cd6130 FS: 00007f3b823f16c0(0000) GS:ffff8880b9400000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f3b823f0ff8 CR3: 000000004674a000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __inet_hash_connect+0x140f/0x20b0 net/ipv4/inet_hashtables.c:1139 dccp_v6_connect+0xcb9/0x1480 net/dccp/ipv6.c:956 __inet_stream_connect+0x262/0xf30 net/ipv4/af_inet.c:678 inet_stream_connect+0x65/0xa0 net/ipv4/af_inet.c:749 __sys_connect_file net/socket.c:2048 [inline] __sys_connect+0x2df/0x310 net/socket.c:2065 __do_sys_connect net/socket.c:2075 [inline] __se_sys_connect net/socket.c:2072 [inline] __x64_sys_connect+0x7a/0x90 net/socket.c:2072 do_syscall_64+0xf9/0x240 entry_SYSCALL_64_after_hwframe+0x6f/0x77 RIP: 0033:0x7f3b8167dda9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 e1 20 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f3b823f10c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002a RAX: ffffffffffffffda RBX: 00007f3b817abf80 RCX: 00007f3b8167dda9 RDX: 000000000000001c RSI: 0000000020000040 RDI: 0000000000000003 RBP: 00007f3b823f1120 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000001 R13: 000000000000000b R14: 00007f3b817abf80 R15: 00007ffd3beb57b8 </TASK> | 5.9 | More Details |
| CVE-2024-32745 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the PAGE DESCRIPTION parameter under the CURRENT PAGE module. | 5.9 | More Details |
| CVE-2024-32591 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daniele De Rosa Backend Designer allows Stored XSS.This issue affects Backend Designer: from n/a through 1.3. | 5.9 | More Details |
| CVE-2024-32320 | Tenda AC500 V2.0.1.9(1307) firmware has a stack overflow vulnerability via the timeZone parameter in the formSetTimeZone function. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32126 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Peters Navigation menu as Dropdown Widget allows Stored XSS.This issue affects Navigation menu as Dropdown Widget: from n/a through 1.3.4. | 5.9 | More Details |
| CVE-2024-32597 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xylus Themes WordPress Importer allows Stored XSS.This issue affects WordPress Importer: from n/a through 1.0.7. | 5.9 | More Details |
| CVE-2024-30979 | Cross Site Scripting vulnerability in Cyber Cafe Management System 1.0 allows a remote attacker to execute arbitrary code via the compname parameter in edit-computer-details.php. | 5.9 | More Details |
| CVE-2024-32534 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 10Web Form Builder Team Form Maker by 10Web allows Stored XSS.This issue affects Form Maker by 10Web: from n/a through 1.15.23. | 5.9 | More Details |
| CVE-2023-5398 | Server receiving a malformed message based on a list of IPs resulting in heap corruption causing a denial of service. See Honeywell Security Notification for recommendations on upgrading and versioning. | 5.9 | More Details |
| CVE-2023-5405 | Server information leak for the CDA Server process memory can occur when an error is generated in response to a specially crafted message. See Honeywell Security Notification for recommendations on upgrading and versioning. | 5.9 | More Details |
| CVE-2024-32540 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Web357 Fixed HTML Toolbar allows Stored XSS.This issue affects Fixed HTML Toolbar: from n/a through 1.0.7. | 5.9 | More Details |
| CVE-2024-32573 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for eBay allows Stored XSS.This issue affects WP-Lister Lite for eBay: from n/a through 3.5.11. | 5.9 | More Details |
| CVE-2023-5406 | Server communication with a controller can lead to remote code execution using a specially crafted message from the controller. See Honeywell Security Notification for recommendations on upgrading and versioning. | 5.9 | More Details |
| CVE-2023-5407 | Controller denial of service due to improper handling of a specially crafted message received by the controller. See Honeywell Security Notification for recommendations on upgrading and versioning. | 5.9 | More Details |
| CVE-2024-32584 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StandaloneTech TeraWallet – For WooCommerce allows Stored XSS.This issue affects TeraWallet – For WooCommerce: from n/a through 1.5.0. | 5.9 | More Details |
| CVE-2024-32598 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Booking Algorithms BA Book Everything allows Stored XSS.This issue affects BA Book Everything: from n/a through 1.6.8. | 5.9 | More Details |
| CVE-2024-3470 | An Improper Privilege Management vulnerability was identified in GitHub Enterprise Server that allowed an attacker to use a deploy key pertaining to an organization to bypass an organization ruleset. An attacker would require access to a valid deploy key for a repository in the organization as well as repository administrator access. This vulnerability affected versions of GitHub Enterprise Server 3.11 to 3.12 and was fixed in versions 3.11.8 and 3.12.2. This vulnerability was reported via the GitHub Bug Bounty program. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32548 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hideki Tanaka What's New Generator allows Stored XSS.This issue affects What's New Generator: from n/a through 2.0.2. | 5.9 | More Details |
| CVE-2024-32690 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fahad Mahmood RSS Feed Widget allows Stored XSS.This issue affects RSS Feed Widget: from n/a through 2.9.7. | 5.9 | More Details |
| CVE-2024-32547 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Max Bond Code Insert Manager (Q2W3 Inc Manager) allows Reflected XSS.This issue affects Code Insert Manager (Q2W3 Inc Manager): from n/a through 2.5.3. | 5.8 | More Details |
| CVE-2024-29028 | memos is a privacy-first, lightweight note-taking service. In memos 0.13.2, an SSRF vulnerability exists at the /o/get/httpmeta that allows unauthenticated users to enumerate the internal network and receive limited html values in json form. This vulnerability is fixed in 0.16.1. | 5.8 | More Details |
| CVE-2024-29030 | memos is a privacy-first, lightweight note-taking service. In memos 0.13.2, an SSRF vulnerability exists at the /api/resource that allows authenticated users to enumerate the internal network. Version 0.22.0 of memos removes the vulnerable file. | 5.8 | More Details |
| CVE-2024-29964 | Brocade SANnav versions before v2.3.0a do not correctly set permissions on files, including docker files. An unprivileged attacker who gains access to the server can read sensitive information from these files. | 5.7 | More Details |
| CVE-2024-29951 | Brocade SANnav before v2.3.1 and v2.3.0a uses the SHA-1 hash in internal SSH ports that are not open to remote connection. | 5.7 | More Details |
| CVE-2024-32306 | Tenda AC10U v1.0 Firmware v15.03.06.49 has a stack overflow vulnerability located via the PPW parameter in the fromWizardHandle function. | 5.7 | More Details |
| CVE-2024-2101 | The Salon booking system WordPress plugin before 9.6.3 does not properly sanitize and escape the 'Mobile Phone' field when booking an appointment, allowing customers to conduct Stored Cross-Site Scripting attacks. The payload gets triggered when an admin visits the 'Customers' page and the malicious script is executed in the admin context. | 5.7 | More Details |
| CVE-2024-32312 | Tenda F1203 V2.0.1.6 firmware has a stack overflow vulnerability located in the adslPwd parameter of the formWanParameterSetting function. | 5.7 | More Details |
| CVE-2024-30800 | PX4 Autopilot v.1.14 allows an attacker to fly the drone into no-fly zones by breaching the geofence using flaws in the function. | 5.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26899 | In the Linux kernel, the following vulnerability has been resolved: block: fix deadlock between bd_link_disk_holder and partition scan 'open_mutex' of gendisk is used to protect open/close block devices. But in bd_link_disk_holder(), it is used to protect the creation of symlink between holding disk and slave bdev, which introduces some issues. When bd_link_disk_holder() is called, the driver is usually in the process of initialization/modification and may suspend submitting io. At this time, any io hold 'open_mutex', such as scanning partitions, can cause deadlocks. For example, in raid: T1 T2 bdev_open_by_dev lock open_mutex [1] ... efi_partition ... md_submit_bio md_ioctl mddev_syspend -> suspend all io md_add_new_disk bind_rdev_to_array bd_link_disk_holder try lock open_mutex [2] md_handle_request -> wait mddev_resume T1 scan partition, T2 add a new device to raid. T1 waits for T2 to resume mddev, but T2 waits for open_mutex held by T1. Deadlock occurs. Fix it by introducing a local mutex 'blk_holder_mutex' to replace 'open_mutex'. | 5.5 | More Details |
| CVE-2023-22869 | IBM Aspera Faspex 5.0.0 through 5.0.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 244119. | 5.5 | More Details |
| CVE-2023-38299 | Various software builds for the AT&T Calypso, Nokia C100, Nokia C200, and BLU View 3 devices leak the device IMEI to a system property that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in these instances they are leaked by a high-privilege process and can be obtained indirectly. The software build fingerprints for each confirmed vulnerable device are as follows: AT&T Calypso (ATT/U318AA/U318AA:10/QP1A.190711.020/1632369780:user/release-keys); Nokia C100 (Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_190:user/release-keys and Nokia/DrakeLite_02US/DKT:12/SP1A.210812.016/02US_1_270:user/release-keys); Nokia C200 (Nokia/Drake_02US/DRK:12/SP1A.210812.016/02US_1_080:user/release-keys); and BLU View 3 (BLU/B140DL/B140DL:11/RP1A.200720.011/1628014629:user/release-keys, BLU/B140DL/B140DL:11/RP1A.200720.011/1632535579:user/release-keys, BLU/B140DL/B140DL:11/RP1A.200720.011/1637325978:user/release-keys, BLU/B140DL/B140DL:11/RP1A.200720.011/1650073052:user/release-keys, BLU/B140DL/B140DL:11/RP1A.200720.011/1657087912:user/release-keys, BLU/B140DL/B140DL:11/RP1A.200720.011/1666316280:user/release-keys, and BLU/B140DL/B140DL:11/RP1A.200720.011/1672371162:user/release-keys). This malicious app reads from the "persist.sys.imei1" system property to indirectly obtain the device IMEI. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26902 | In the Linux kernel, the following vulnerability has been resolved: perf: RISCV: Fix panic on pmu overflow handler (1 << idx) of int is not desired when setting bits in unsigned long overflowed_ctrs, use BIT() instead. This panic happens when running 'perf record -e branches' on sophgo sg2042. [ 273.311852] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000098 [ 273.320851] Oops [#1] [ 273.323179] Modules linked in: [ 273.326303] CPU: 0 PID: 1475 Comm: perf Not tainted 6.6.0-rc3+ #9 [ 273.332521] Hardware name: Sophgo Mango (DT) [ 273.336878] epc : riscv_pmu_ctr_get_width_mask+0x8/0x62 [ 273.342291] ra : pmu_sbi_ovf_handler+0x2e0/0x34e [ 273.347091] epc : ffffffff80aecd98 ra : ffffffff80aee056 sp : ffffff6e36928b0 [ 273.354454] gp : ffffffff821f82d0 tp : ffffffd90c353200 t0 : 0000002ade4f9978 [ 273.361815] t1 : 0000000000504d55 t2 : ffffffff8016cd8c s0 : ffffff6e3692a70 [ 273.369180] s1 : 0000000000000020 a0 : 0000000000000000 a1 : 00001a8e81800000 [ 273.376540] a2 : 0000003c00070198 a3 : 0000003c00db75a4 a4 : 0000000000000015 [ 273.383901] a5 : ffffffd7ff8804b0 a6 : 0000000000000015 a7 : 000000000000002a [ 273.391327] s2 : 000000000000ffff s3 : 0000000000000000 s4 : ffffffd7ff8803b0 [ 273.398773] s5 : 0000000000504d55 s6 : ffffffd905069800 s7 : ffffffff821fe210 [ 273.406139] s8 : 000000007fffffff s9 : ffffffd7ff8803b0 s10: ffffffd903f29098 [ 273.413660] s11: 0000000080000000 t3 : 0000000000000003 t4 : ffffffff8017a0ca [ 273.421022] t5 : ffffffff8023cfc2 t6 : ffffffd9040780e8 [ 273.426437] status: 0000000200000100 badaddr: 0000000000000098 cause: 000000000000000d [ 273.434512] [<ffffffff80aecd98>] riscv_pmu_ctr_get_width_mask+0x8/0x62 [ 273.441169] [<ffffffff80076bd8>] handle_percpu_devid_irq+0x98/0x1ee [ 273.447562] [<ffffffff80071158>] generic_handle_domain_irq+0x28/0x36 [ 273.454151] [<ffffffff8047a99a>] riscv_intc_irq+0x36/0x4e [ 273.459659] [<ffffffff80c944de>] handle_riscv_irq+0x4a/0x74 [ 273.465442] [<ffffffff80c94c48>] do_irq+0x62/0x92 [ 273.470360] Code: 0420 60a2 6402 5529 0141 8082 0013 0000 0013 0000 (6d5c) b783 [ 273.477921] ---[ end trace 0000000000000000 ]--- [ 273.482630] Kernel panic - not syncing: Fatal exception in interrupt | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26881 | In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when 1588 is received on HIP08 devices The HIP08 devices does not register the ptp devices, so the hdev->ptp is NULL, but the hardware can receive 1588 messages, and set the HNS3_RXD_TS_VLD_B bit, so, if match this case, the access of hdev->ptp->flags will cause a kernel crash: [ 5888.946472] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 [ 5888.946475] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000018 ... [ 5889.266118] pc : hclge_ptp_get_rx_hwts+0x40/0x170 [hclge] [ 5889.272612] lr : hclge_ptp_get_rx_hwts+0x34/0x170 [hclge] [ 5889.279101] sp : ffff800012c3bc50 [ 5889.283516] x29: ffff800012c3bc50 x28: ffff2040002be040 [ 5889.289927] x27: ffff800009116484 x26: 0000000080007500 [ 5889.296333] x25: 0000000000000000 x24: ffff204001c6f000 [ 5889.302738] x23: ffff204144f53c00 x22: 0000000000000000 [ 5889.309134] x21: 0000000000000000 x20: ffff204004220080 [ 5889.315520] x19: ffff204144f53c00 x18: 0000000000000000 [ 5889.321897] x17: 0000000000000000 x16: 0000000000000000 [ 5889.328263] x15: 0000004000140ec8 x14: 0000000000000000 [ 5889.334617] x13: 0000000000000000 x12: 00000000010011df [ 5889.340965] x11: bbfeff4d22000000 x10: 0000000000000000 [ 5889.347303] x9 : ffff800009402124 x8 : 0200f78811dfbb4d [ 5889.353637] x7 : 2200000000191b01 x6 : ffff208002a7d480 [ 5889.359959] x5 : 0000000000000000 x4 : 0000000000000000 [ 5889.366271] x3 : 0000000000000000 x2 : 0000000000000000 [ 5889.372567] x1 : 0000000000000000 x0 : ffff20400095c080 [ 5889.378857] Call trace: [ 5889.382285] hclge_ptp_get_rx_hwts+0x40/0x170 [hclge] [ 5889.388304] hns3_handle_bdinfo+0x324/0x410 [hns3] [ 5889.394055] hns3_handle_rx_bd+0x60/0x150 [hns3] [ 5889.399624] hns3_clean_rx_ring+0x84/0x170 [hns3] [ 5889.405270] hns3_nic_common_poll+0xa8/0x220 [hns3] [ 5889.411084] napi_poll+0xcc/0x264 [ 5889.415329] net_rx_action+0xd4/0x21c [ 5889.419911] __do_softirq+0x130/0x358 [ 5889.424484] irq_exit+0x134/0x154 [ 5889.428700] __handle_domain_irq+0x88/0xf0 [ 5889.433684] gic_handle_irq+0x78/0x2c0 [ 5889.438319] el1_irq+0xb8/0x140 [ 5889.442354] arch_cpu_idle+0x18/0x40 [ 5889.446816] default_idle_call+0x5c/0x1c0 [ 5889.451714] cpuidle_idle_call+0x174/0x1b0 [ 5889.456692] do_idle+0xc8/0x160 [ 5889.460717] cpu_startup_entry+0x30/0xfc [ 5889.465523] secondary_start_kernel+0x158/0x1ec [ 5889.470936] Code: 97ffab78 f9411c14 91408294 f9457284 (f9400c80) [ 5889.477950] SMP: stopping secondary CPUs [ 5890.514626] SMP: failed to stop secondary CPUs 0-69,71-95 [ 5890.522951] Starting crashdump kernel... | 5.5 | More Details |
| CVE-2024-26900 | In the Linux kernel, the following vulnerability has been resolved: md: fix kmemleak of rdev->serial If kobject_add() is fail in bind_rdev_to_array(), 'rdev->serial' will be alloc not be freed, and kmemleak occurs. unreferenced object 0xffff88815a350000 (size 49152): comm "mdadm", pid 789, jiffies 4294716910 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc f773277a): [<0000000058b0a453>] kmemleak_alloc+0x61/0xe0 [<00000000366adf14>] __kmalloc_large_node+0x15e/0x270 [<000000002e82961b>] __kmalloc_node.cold+0x11/0x7f [<00000000f206d60a>] kvmalloc_node+0x74/0x150 [<0000000034bf3363>] rdev_init_serial+0x67/0x170 [<0000000010e08fe9>] mddev_create_serial_pool+0x62/0x220 [<00000000c3837bf0>] bind_rdev_to_array+0x2af/0x630 [<0000000073c28560>] md_add_new_disk+0x400/0x9f0 [<00000000770e30ff>] md_ioctl+0x15bf/0x1c10 [<000000006cfab718>] blkdev_ioctl+0x191/0x3f0 [<0000000085086a11>] vfs_ioctl+0x22/0x60 [<0000000018b656fe>] __x64_sys_ioctl+0xba/0xe0 [<00000000e54e675e>] do_syscall_64+0x71/0x150 [<000000008b0ad622>] entry_SYSCALL_64_after_hwframe+0x6c/0x74 | 5.5 | More Details |
| CVE-2024-26889 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Fix possible buffer overflow struct hci_dev_info has a fixed size name[8] field so in the event that hdev->name is bigger than that strcpy would attempt to write past its size, so this fixes this problem by switching to use strscpy. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3838 | Inappropriate implementation in Autofill in Google Chrome prior to 124.0.6367.60 allowed an attacker who convinced a user to install a malicious app to perform UI spoofing via a crafted app. (Chromium security severity: Medium) | 5.5 | More Details |
| CVE-2024-26915 | In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Reset IH OVERFLOW_CLEAR bit Allows us to detect subsequent IH ring buffer overflows as well. | 5.5 | More Details |
| CVE-2024-32327 | TOTOLINK N300RT V2.1.8-B20201030.1539 contains a Store Cross-site scripting (XSS) vulnerability in Port Forwarding under the Firewall Page. | 5.5 | More Details |
| CVE-2024-29962 | Brocade SANnav OVA before v2.3.1 and v2.3.0a have an insecure file permission setting that makes files world-readable. This could allow a local user without the required privileges to access sensitive information or a Java binary. | 5.5 | More Details |
| CVE-2024-26903 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: rfcomm: Fix null-ptr-deref in rfcomm_check_security During our fuzz testing of the connection and disconnection process at the RFCOMM layer, we discovered this bug. By comparing the packets from a normal connection and disconnection process with the testcase that triggered a KASAN report. We analyzed the cause of this bug as follows: 1. In the packets captured during a normal connection, the host sends a `Read Encryption Key Size` type of `HCI_CMD` packet (Command Opcode: 0x1408) to the controller to inquire the length of encryption key.After receiving this packet, the controller immediately replies with a Command Completepacket (Event Code: 0x0e) to return the Encryption Key Size. 2. In our fuzz test case, the timing of the controller's response to this packet was delayed to an unexpected point: after the RFCOMM and L2CAP layers had disconnected but before the HCI layer had disconnected. 3. After receiving the Encryption Key Size Response at the time described in point 2, the host still called the rfcomm_check_security function. However, by this time `struct l2cap_conn *conn = l2cap_pi(sk)->chan->conn;` had already been released, and when the function executed `return hci_conn_security(conn->hcon, d->sec_level, auth_type, d->out);`, specifically when accessing `conn->hcon`, a null-ptr-deref error occurred. To fix this bug, check if `sk->sk_state` is BT_CLOSED before calling rfcomm_recv_frame in rfcomm_process_rx. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26909 | In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink_altmode: fix drm bridge use-after-free A recent DRM series purporting to simplify support for "transparent bridges" and handling of probe deferrals ironically exposed a use-after-free issue on pmic_glink_altmode probe deferral. This has manifested itself as the display subsystem occasionally failing to initialise and NULL-pointer dereferences during boot of machines like the Lenovo ThinkPad X13s. Specifically, the dp-hpd bridge is currently registered before all resources have been acquired which means that it can also be deregistered on probe deferrals. In the meantime there is a race window where the new aux bridge driver (or PHY driver previously) may have looked up the dp-hpd bridge and stored a (non-reference-counted) pointer to the bridge which is about to be deallocated. When the display controller is later initialised, this triggers a use-after-free when attaching the bridges: dp -> aux -> dp-hpd (freed) which may, for example, result in the freed bridge failing to attach: [drm:drm_bridge_attach [drm]] *ERROR* failed to attach bridge /soc@0/phy@88eb000 to encoder TMDS-31: -16 or a NULL-pointer dereference: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 ... Call trace: drm_bridge_attach+0x70/0x1a8 [drm] drm_aux_bridge_attach+0x24/0x38 [aux_bridge] drm_bridge_attach+0x80/0x1a8 [drm] dp_bridge_init+0xa8/0x15c [msm] msm_dp_modeset_init+0x28/0xc4 [msm] The DRM bridge implementation is clearly fragile and implicitly built on the assumption that bridges may never go away. In this case, the fix is to move the bridge registration in the pmic_glink_altmode driver to after all resources have been looked up. Incidentally, with the new dp-hpd bridge implementation, which registers child devices, this is also a requirement due to a long-standing issue in driver core that can otherwise lead to a probe deferral loop (see commit fbc35b45f9f6 ("Add documentation on meaning of -EPROBE_DEFER")). [DB: slightly fixed commit message by adding the word 'commit'] | 5.5 | More Details |
| CVE-2024-26912 | In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: fix several DMA buffer leaks Nouveau manages GSP-RM DMA buffers with nvkm_gsp_mem objects. Several of these buffers are never dealloced. Some of them can be deallocated right after GSP-RM is initialized, but the rest need to stay until the driver unloads. Also futher bullet-proof these objects by poisoning the buffer and clearing the nvkm_gsp_mem object when it is deallocated. Poisoning the buffer should trigger an error (or crash) from GSP-RM if it tries to access the buffer after we've deallocated it, because we were wrong about when it is safe to deallocate. Finally, change the mem->size field to a size_t because that's the same type that dma_alloc_coherent expects. | 5.5 | More Details |
| CVE-2024-31584 | Pytorch before v2.2.0 has an Out-of-bounds Read vulnerability via the component torch/csrc/jit/mobile/flatbuffer_loader.cpp. | 5.5 | More Details |
| CVE-2024-32743 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the SITE LANGUAGE CONFIG parameter under the Security module. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26901 | In the Linux kernel, the following vulnerability has been resolved: do_sys_name_to_handle(): use kzalloc() to fix kernel-infoleak syzbot identified a kernel information leak vulnerability in do_sys_name_to_handle() and issued the following report [1]. [1] "BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_user+0xbc/0x100 lib/usercopy.c:40 instrument_copy_to_user include/linux/instrumented.h:114 [inline] _copy_to_user+0xbc/0x100 lib/usercopy.c:40 copy_to_user include/linux/uaccess.h:191 [inline] do_sys_name_to_handle fs/fhandle.c:73 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x949/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc+0x121/0x3c0 mm/slab_common.c:1020 kmalloc include/linux/slab.h:604 [inline] do_sys_name_to_handle fs/fhandle.c:39 [inline] __do_sys_name_to_handle_at fs/fhandle.c:112 [inline] __se_sys_name_to_handle_at+0x441/0xb10 fs/fhandle.c:94 __x64_sys_name_to_handle_at+0xe4/0x140 fs/fhandle.c:94 ... Bytes 18-19 of 20 are uninitialized Memory access of size 20 starts at ffff888128a46380 Data copied to user address 0000000020000240" Per Chuck Lever's suggestion, use kzalloc() instead of kmalloc() to solve the problem. | 5.5 | More Details |
| CVE-2024-2440 | A race condition in GitHub Enterprise Server allowed an existing admin to maintain permissions on a detached repository by making a GraphQL mutation to alter repository permissions while the repository is detached. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.13 and was fixed in versions 3.9.13, 3.10.10, 3.11.8 and 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program. | 5.5 | More Details |
| CVE-2024-1241 | Watchdog Antivirus v1.6.415 is vulnerable to a Denial of Service vulnerability by triggering the 0x80002014 IOCTL code of the wsdk-driver.sys driver. | 5.5 | More Details |
| CVE-2024-29952 | A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a could allow an authenticated user to print the Auth, Priv, and SSL key store passwords in unencrypted logs by manipulating command variables. | 5.5 | More Details |
| CVE-2024-31229 | Server-Side Request Forgery (SSRF) vulnerability in Really Simple Plugins Really Simple SSL.This issue affects Really Simple SSL: from n/a through 7.2.3. | 5.5 | More Details |
| CVE-2024-2760 | Bkav Home v7816, build 2403161130 is vulnerable to a Memory Information Leak vulnerability by triggering the 0x222240 IOCTL code of the BkavSDFlt.sys driver. | 5.5 | More Details |
| CVE-2022-40745 | IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain sensitive information due to weaker than expected security. IBM X-Force ID: 236452. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26857 | In the Linux kernel, the following vulnerability has been resolved: geneve: make sure to pull inner header in geneve_rx() syzbot triggered a bug in geneve_rx() [1] Issue is similar to the one I fixed in commit 8d975c15c0cd ("ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv()") We have to save skb->network_header in a temporary variable in order to be able to recompute the network_header pointer after a pskb_inet_may_pull() call. pskb_inet_may_pull() makes sure the needed headers are in skb->head. [1] BUG: KMSAN: uninit-value in IP_ECN_decapsulate include/net/inet_ecn.h:302 [inline] BUG: KMSAN: uninit-value in geneve_rx drivers/net/geneve.c:279 [inline] BUG: KMSAN: uninit-value in geneve_udp_encap_recv+0x36f9/0x3c10 drivers/net/geneve.c:391 IP_ECN_decapsulate include/net/inet_ecn.h:302 [inline] geneve_rx drivers/net/geneve.c:279 [inline] geneve_udp_encap_recv+0x36f9/0x3c10 drivers/net/geneve.c:391 udp_queue_rcv_one_skb+0x1d39/0x1f20 net/ipv4/udp.c:2108 udp_queue_rcv_skb+0x6ae/0x6e0 net/ipv4/udp.c:2186 udp_unicast_rcv_skb+0x184/0x4b0 net/ipv4/udp.c:2346 __udp4_lib_rcv+0x1c6b/0x3010 net/ipv4/udp.c:2422 udp_rcv+0x7d/0xa0 net/ipv4/udp.c:2604 ip_protocol_deliver_rcu+0x264/0x1300 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x2b8/0x440 net/ipv4/ip_input.c:233 NF_HOOK include/linux/netfilter.h:314 [inline] ip_local_deliver+0x21f/0x490 net/ipv4/ip_input.c:254 dst_input include/net/dst.h:461 [inline] ip_rcv_finish net/ipv4/ip_input.c:449 [inline] NF_HOOK include/linux/netfilter.h:314 [inline] ip_rcv+0x46f/0x760 net/ipv4/ip_input.c:569 __netif_receive_skb_one_core net/core/dev.c:5534 [inline] __netif_receive_skb+0x1a6/0x5a0 net/core/dev.c:5648 process_backlog+0x480/0x8b0 net/core/dev.c:5976 __napi_poll+0xe3/0x980 net/core/dev.c:6576 napi_poll net/core/dev.c:6645 [inline] net_rx_action+0x8b8/0x1870 net/core/dev.c:6778 __do_softirq+0x1b7/0x7c5 kernel/softirq.c:553 do_softirq+0x9a/0xf0 kernel/softirq.c:454 __local_bh_enable_ip+0x9b/0xa0 kernel/softirq.c:381 local_bh_enable include/linux/bottom_half.h:33 [inline] rcu_read_unlock_bh include/linux/rcupdate.h:820 [inline] __dev_queue_xmit+0x2768/0x51c0 net/core/dev.c:4378 dev_queue_xmit include/linux/netdevice.h:3171 [inline] packet_xmit+0x9c/0x6b0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3081 [inline] packet_sendmsg+0x8aef/0x9f10 net/packet/af_packet.c:3113 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] __sys_sendto+0x735/0xa10 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x125/0x1c0 net/socket.c:2199 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: slab_post_alloc_hook mm/slub.c:3819 [inline] slab_alloc_node mm/slub.c:3860 [inline] kmem_cache_alloc_node+0x5cb/0xbc0 mm/slub.c:3903 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:560 __alloc_skb+0x352/0x790 net/core/skbuff.c:651 alloc_skb include/linux/skbuff.h:1296 [inline] alloc_skb_with_frags+0xc8/0xbd0 net/core/skbuff.c:6394 sock_alloc_send_pskb+0xa80/0xbf0 net/core/sock.c:2783 packet_alloc_skb net/packet/af_packet.c:2930 [inline] packet_snd net/packet/af_packet.c:3024 [inline] packet_sendmsg+0x70c2/0x9f10 net/packet/af_packet.c:3113 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] __sys_sendto+0x735/0xa10 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x125/0x1c0 net/socket.c:2199 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-1730 | The Prime Slider – Addons For Elementor (Revolution of a slider, Hero Slider, Media Slider, Drag Drop Slider, Video Slider, Product Slider, Ecommerce Slider) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via urls in link fields, images from URLs, and html tags used in widgets in all versions up to, and including, 3.14.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 5.4 | More Details |
| CVE-2024-32515 | Missing Authorization vulnerability in Qamar Sheeraz, Nasir Ahmad Mega Addons For Elementor.This issue affects Mega Addons For Elementor: from n/a through 1.8. | 5.4 | More Details |
| CVE-2024-31857 | Forminator prior to 1.15.4 contains a cross-site scripting vulnerability. If this vulnerability is exploited, a remote attacker may obtain user information etc. and alter the page contents on the user's web browser. | 5.4 | More Details |
| CVE-2024-30886 | A stored cross-site scripting (XSS) vulnerability in the remotelink function of HadSky v7.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter. | 5.4 | More Details |
| CVE-2023-47731 | IBM QRadar Suite Software 1.10.12.0 through 1.10.19.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 272203. | 5.4 | More Details |
| CVE-2024-3818 | The Essential Blocks – Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's "Social Icons" block in all versions up to, and including, 4.5.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 5.4 | More Details |
| CVE-2024-32506 | Exposure of Sensitive Information to an Unauthorized Actor vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73. | 5.4 | More Details |
| CVE-2024-22856 | A SQL injection vulnerability via the Save Favorite Search function in Axefinance Axe Credit Portal >= v.3.0 allows authenticated attackers to execute unintended queries and disclose sensitive information from DB tables via crafted requests. | 5.4 | More Details |
| CVE-2024-27752 | Cross Site Scripting vulnerability in CSZ CMS v.1.3.0 allows a remote attacker to execute arbitrary code via the Default Keyword field in the settings function. | 5.4 | More Details |
| CVE-2024-32338 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the PAGE TITLE parameter under the Current Page module. | 5.4 | More Details |
| CVE-2024-21990 | ONTAP Select Deploy administration utility versions 9.12.1.x, 9.13.1.x and 9.14.1.x contain hard-coded credentials that could allow an attacker to view Deploy configuration information and modify the account credentials. | 5.4 | More Details |
| CVE-2024-29986 | Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32335 | TOTOLINK N300RT V2.1.8-B20201030.1539 contains a Store Cross-site scripting (XSS) vulnerability in Access Control under the Wireless Page. | 5.4 | More Details |
| CVE-2024-30921 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows a remote attacker to execute arbitrary code via the photo.php component. | 5.4 | More Details |
| CVE-2024-32142 | Missing Authorization vulnerability in Ovic Team Ovic Responsive WPBakery.This issue affects Ovic Responsive WPBakery: from n/a through 1.3.0. | 5.4 | More Details |
| CVE-2022-46897 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The CapsuleIFWUSmm driver does not check the return value from a method or function. This can prevent it from detecting unexpected states and conditions. | 5.3 | More Details |
| CVE-2024-32518 | Missing Authorization vulnerability in Pepro Dev. Group PeproDev Ultimate Invoice.This issue affects PeproDev Ultimate Invoice: from n/a through 2.0.0. | 5.3 | More Details |
| CVE-2023-45209 | An information disclosure vulnerability exists in the web interface /cgi-bin/download_config.cgi functionality of Peplink Smart Reader v1.2.0 (in QEMU). A specially crafted HTTP request can lead to a disclosure of sensitive information. An attacker can make an unauthenticated HTTP request to trigger this vulnerability. | 5.3 | More Details |
| CVE-2024-32679 | Missing Authorization vulnerability in Shared Files PRO Shared Files.This issue affects Shared Files: from n/a through 1.7.16. | 5.3 | More Details |
| CVE-2024-1350 | Missing Authorization vulnerability in Prasidhda Malla Honeypot for WP Comment.This issue affects Honeypot for WP Comment: from n/a through 2.2.3. | 5.3 | More Details |
| CVE-2024-4021 | A vulnerability was found in Keenetic KN-1010, KN-1410, KN-1711, KN-1810 and KN-1910 up to 4.1.2.15. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /ndmComponents.js of the component Configuration Setting Handler. The manipulation leads to information disclosure. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261673 was assigned to this vulnerability. NOTE: The vendor is aware of this issue and plans to fix it by the end of 2024. | 5.3 | More Details |
| CVE-2024-32513 | Insertion of Sensitive Information into Log File vulnerability in AdTribes.Io Product Feed PRO for WooCommerce.This issue affects Product Feed PRO for WooCommerce: from n/a through 13.3.1. | 5.3 | More Details |
| CVE-2024-32683 | Authorization Bypass Through User-Controlled Key vulnerability in Wpmet Wp Ultimate Review.This issue affects Wp Ultimate Review: from n/a through 2.2.5. | 5.3 | More Details |
| CVE-2024-24856 | The memory allocation function ACPI_ALLOCATE_ZEROED does not guarantee a successful allocation, but the subsequent code directly dereferences the pointer that receives it, which may lead to null pointer dereference. To fix this issue, a null pointer check should be added. If it is null, return exception code AE_NO_MEMORY. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-31585 | FFmpeg version n5.1 to n6.1 was discovered to contain an Off-by-one Error vulnerability in libavfilter/avf_showspectrum.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input. | 5.3 | More Details |
| CVE-2024-32532 | Missing Authorization vulnerability in SiteGround Speed Optimizer.This issue affects Speed Optimizer: from n/a through 7.4.6. | 5.3 | More Details |
| CVE-2024-21846 | An unauthenticated attacker can reset the board and stop transmitter operations by sending a specially-crafted GET request to the command.cgi gateway, resulting in a denial-of-service scenario. | 5.3 | More Details |
| CVE-2024-4022 | A vulnerability was found in Keenetic KN-1010, KN-1410, KN-1711, KN-1810 and KN-1910 up to 4.1.2.15. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /version.js of the component Version Data Handler. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-261674 is the identifier assigned to this vulnerability. NOTE: The vendor is aware of this issue and plans to fix it by the end of 2024. | 5.3 | More Details |
| CVE-2024-32601 | Missing Authorization vulnerability in WP OnlineSupport, Essential Plugin Popup Anything.This issue affects Popup Anything: from n/a through 2.8. | 5.3 | More Details |
| CVE-2024-28890 | Forminator prior to 1.29.0 contains an unrestricted upload of file with dangerous type vulnerability. If this vulnerability is exploited, a remote attacker may obtain sensitive information by accessing files on the server, alter the site that uses the plugin, and cause a denial-of-service (DoS) condition. | 5.3 | More Details |
| CVE-2024-27347 | Server-Side Request Forgery (SSRF) vulnerability in Apache HugeGraph-Hubble.This issue affects Apache HugeGraph-Hubble: from 1.0.0 before 1.3.0. Users are recommended to upgrade to version 1.3.0, which fixes the issue. | 5.3 | More Details |
| CVE-2024-21972 | An out of bounds write vulnerability in the AMD Radeon™ user mode driver for DirectX® 11 could allow an attacker with access to a malformed shader to potentially achieve arbitrary code execution. | 5.3 | More Details |
| CVE-2024-1219 | The Easy Social Feed WordPress plugin before 6.5.6 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin | 5.3 | More Details |
| CVE-2024-32686 | Insertion of Sensitive Information into Log File vulnerability in Inisev Backup Migration.This issue affects Backup Migration: from n/a through 1.4.3. | 5.3 | More Details |
| CVE-2023-7252 | The Tickera WordPress plugin before 3.5.2.5 does not prevent users from leaking other users' tickets. | 5.3 | More Details |
| CVE-2024-32684 | Missing Authorization vulnerability in Wpmet Wp Ultimate Review.This issue affects Wp Ultimate Review: from n/a through 2.2.5. | 5.3 | More Details |
| CVE-2024-32691 | Missing Authorization vulnerability in realmag777 Active Products Tables for WooCommerce.This issue affects Active Products Tables for WooCommerce: from n/a through 1.0.6.2. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-22815 | An issue in the communication protocol of Tormach xsTECH CNC Router, PathPilot Controller v2.9.6 allows attackers to cause a Denial of Service (DoS) via crafted commands. | 5.3 | More Details |
| CVE-2024-32869 | Hono is a Web application framework that provides support for any JavaScript runtime. Prior to version 4.2.7, when using serveStatic with deno, it is possible to traverse the directory where `main.ts` is located. This can result in retrieval of unexpected files. Version 4.2.7 contains a patch for the issue. | 5.3 | More Details |
| CVE-2024-0868 | The coreActivity: Activity Logging plugin for WordPress plugin before 2.1 retrieved IP addresses of requests via headers such X-FORWARDED to log them, allowing users to spoof them by providing an arbitrary value | 5.3 | More Details |
| CVE-2024-21979 | An out of bounds write vulnerability in the AMD Radeon™ user mode driver for DirectX® 11 could allow an attacker with access to a malformed shader to potentially achieve arbitrary code execution. | 5.3 | More Details |
| CVE-2023-43491 | An information disclosure vulnerability exists in the web interface /cgi-bin/debug_dump.cgi functionality of Peplink Smart Reader v1.2.0 (in QEMU). A specially crafted HTTP request can lead to a disclosure of sensitive information. An attacker can make an unauthenticated HTTP request to trigger this vulnerability. | 5.3 | More Details |
| CVE-2024-26847 | In the Linux kernel, the following vulnerability has been resolved: powerpc/rtas: use correct function name for resetting TCE tables The PAPR spec spells the function name as "ibm,reset-pe-dma-windows" but in practice firmware uses the singular form: "ibm,reset-pe-dma-window" in the device tree. Since we have the wrong spelling in the RTAS function table, reverse lookups (token -> name) fail and warn: unexpected failed lookup for token 86 WARNING: CPU: 1 PID: 545 at arch/powerpc/kernel/rtas.c:659 __do_enter_rtas_trace+0x2a4/0x2b4 CPU: 1 PID: 545 Comm: systemd-udevd Not tainted 6.8.0-rc4 #30 Hardware name: IBM,9105-22A POWER10 (raw) 0x800200 0xf000006 of:IBM,FW1060.00 (NL1060_028) hv:phyp pSeries NIP [c0000000000417f0] __do_enter_rtas_trace+0x2a4/0x2b4 LR [c0000000000417ec] __do_enter_rtas_trace+0x2a0/0x2b4 Call Trace: __do_enter_rtas_trace+0x2a0/0x2b4 (unreliable) rtas_call+0x1f8/0x3e0 enable_ddw.constprop.0+0x4d0/0xc84 dma_iommu_dma_supported+0xe8/0x24c dma_set_mask+0x5c/0xd8 mlx5_pci_init.constprop.0+0xf0/0x46c [mlx5_core] probe_one+0xfc/0x32c [mlx5_core] local_pci_probe+0x68/0x12c pci_call_probe+0x68/0x1ec pci_device_probe+0xbc/0x1a8 really_probe+0x104/0x570 __driver_probe_device+0xb8/0x224 driver_probe_device+0x54/0x130 __driver_attach+0x158/0x2b0 bus_for_each_dev+0xa8/0x120 driver_attach+0x34/0x48 bus_add_driver+0x174/0x304 driver_register+0x8c/0x1c4 __pci_register_driver+0x68/0x7c mlx5_init+0xb8/0x118 [mlx5_core] do_one_initcall+0x60/0x388 do_init_module+0x7c/0x2a4 init_module_from_file+0xb4/0x108 idempotent_init_module+0x184/0x34c sys_finit_module+0x90/0x114 And oopses are possible when lockdep is enabled or the RTAS tracepoints are active, since those paths dereference the result of the lookup. Use the correct spelling to match firmware's behavior, adjusting the related constants to match. | 5.1 | More Details |
| CVE-2023-25043 | Incorrect Authorization vulnerability in Supsystic Data Tables Generator.This issue affects Data Tables Generator: from n/a through 1.10.25. | 5.0 | More Details |
| CVE-2024-29991 | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability | 5.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-29955 | A vulnerability in Brocade SANnav before v2.3.1 and v2.3.0a could allow a privileged user to print the SANnav encrypted key in PostgreSQL startup logs. This could provide attackers with an additional, less-protected path to acquiring the encryption key. | 5.0 | More Details |
| CVE-2024-28717 | An issue in OpenStack Storlets yoga-eom allows a remote attacker to execute arbitrary code via the gateway.py component. | 4.9 | More Details |
| CVE-2024-2309 | The WP STAGING WordPress Backup Plugin WordPress plugin before 3.4.0, wp-staging-pro WordPress plugin before 5.4.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) | 4.8 | More Details |
| CVE-2024-32473 | Moby is an open source container framework that is a key component of Docker Engine, Docker Desktop, and other distributions of container tooling or runtimes. In 26.0.0, IPv6 is not disabled on network interfaces, including those belonging to networks where `--ipv6=false`. An container with an `ipvlan` or `macvlan` interface will normally be configured to share an external network link with the host machine. Because of this direct access, (1) Containers may be able to communicate with other hosts on the local network over link-local IPv6 addresses, (2) if router advertisements are being broadcast over the local network, containers may get SLAAC-assigned addresses, and (3) the interface will be a member of IPv6 multicast groups. This means interfaces in IPv4-only networks present an unexpectedly and unnecessarily increased attack surface. The issue is patched in 26.0.2. To completely disable IPv6 in a container, use `--sysctl=net.ipv6.conf.all.disable_ipv6=1` in the `docker create` or `docker run` command. Or, in the service configuration of a `compose` file. | 4.7 | More Details |
| CVE-2024-2102 | The Salon booking system WordPress plugin before 9.6.3 does not properly sanitize and escape the 'Mobile Phone' field and 'sms_prefix' parameter when booking an appointment, allowing customers to conduct Stored Cross-Site Scripting attacks. The payload gets triggered when an admin visits the 'Bookings' page and the malicious script is executed in the admin context. | 4.7 | More Details |
| CVE-2024-26910 | In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix performance regression in swap operation The patch "netfilter: ipset: fix race condition between swap/destroy and kernel side add/del/test", commit 28628fa9 fixes a race condition. But the synchronize_rcu() added to the swap function unnecessarily slows it down: it can safely be moved to destroy and use call_rcu() instead. Eric Dumazet pointed out that simply calling the destroy functions as rcu callback does not work: sets with timeout use garbage collectors which need cancelling at destroy which can wait. Therefore the destroy functions are split into two: cancelling garbage collectors safely at executing the command received by netlink and moving the remaining part only into the rcu callback. | 4.7 | More Details |
| CVE-2024-32315 | Tenda FH1202 v1.2.0.14(408) firmware has a stack overflow vulnerability via the adslPwd parameter in the formWanParameterSetting function. | 4.7 | More Details |
| CVE-2023-52645 | In the Linux kernel, the following vulnerability has been resolved: pmdomain: mediatek: fix race conditions with genpd If the power domains are registered first with genpd and *after that* the driver attempts to power them on in the probe sequence, then it is possible that a race condition occurs if genpd tries to power them on in the same time. The same is valid for powering them off before unregistering them from genpd. Attempt to fix race conditions by first removing the domains from genpd and *after that* powering down domains. Also first power up the domains and *after that* register them to genpd. | 4.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-31463 | Ironic-image is an OpenStack Ironic deployment packaged and configured by Metal3. When the reverse proxy mode is enabled by the `IRONIC_REVERSE_PROXY_SETUP` variable set to `true`, 1) HTTP basic credentials are validated on the HTTPD side in a separate container, not in the Ironic service itself and 2) Ironic listens in host network on a private port 6388 on localhost by default. As a result, when the reverse proxy mode is used, any Pod or local Unix user on the control plane Node can access the Ironic API on the private port without authentication. A similar problem affects Ironic Inspector (`INSPECTOR_REVERSE_PROXY_SETUP` set to `true`), although the attack potential is smaller there. This issue affects operators deploying ironic-image in the reverse proxy mode, which is the recommended mode when TLS is used (also recommended), with the `IRONIC_PRIVATE_PORT` variable unset or set to a numeric value. In this case, an attacker with enough privileges to launch a pod on the control plane with host networking can access Ironic API and use it to modify bare-metal machine, e.g. provision them with a new image or change their BIOS settings. This vulnerability is fixed in 24.1.1. | 4.7 | More Details |
| CVE-2024-32206 | A stored cross-site scripting (XSS) vulnerability in the component \affiche\admin\index.php of WUZHICMS v4.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the $formdata parameter. | 4.6 | More Details |
| CVE-2024-30924 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows attackers to execute arbitrary code via the checkin.php component. | 4.6 | More Details |
| CVE-2024-30926 | Cross Site Scripting vulnerability in DerbyNet v9.0 and below allows attackers to execute arbitrary code via the ./inc/kiosks.inc component. | 4.6 | More Details |
| CVE-2024-4026 | Cross-Site Scripting (XSS) vulnerability in the Holded application. This vulnerability could allow an attacker to store a JavaScript payload within all editable parameters within the 'General' and 'Team ID' functionalities, which could result in a session takeover. | 4.6 | More Details |
| CVE-2024-29217 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Answer.This issue affects Apache Answer: before 1.3.0. XSS attack when user changes personal website. A logged-in user, when modifying their personal website, can input malicious code in the website to create such an attack. Users are recommended to upgrade to version [1.3.0], which fixes the issue. | 4.6 | More Details |
| CVE-2024-32657 | Hydra is a Continuous Integration service for Nix based projects. Attackers can execute arbitrary code in the browser context of Hydra and execute authenticated HTTP requests. The abused feature allows Nix builds to specify files that Hydra serves to clients. One use of this functionality is serving NixOS `.iso` files. The issue is only with html files served by Hydra. The issue has been patched on https://hydra.nixos.org around 2024-04-21 14:30 UTC. The nixpkgs package were fixed in unstable and 23.11. Users with custom Hydra packages can apply the fix commit to their local installations. The vulnerability is only triggered when opening HTML build artifacts, so not opening them until the vulnerability is fixed works around the issue. | 4.6 | More Details |
| CVE-2024-32746 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the MENU parameter under the Menu module. | 4.6 | More Details |
| CVE-2024-32744 | A cross-site scripting (XSS) vulnerability in the Settings section of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the PAGE KEYWORDS parameter under the CURRENT PAGE module. | 4.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32392 | Cross Site Scripting vulnerability in CmSimple v.5.15 allows a remote attacker to execute arbitrary code via the functions.php component. | 4.5 | More Details |
| CVE-2023-6833 | Insertion of Sensitive Information into Log File vulnerability in Hitachi Ops Center Administrator allows local users to gain sensitive information.This issue affects Hitachi Ops Center Administrator: before 11.0.1. | 4.4 | More Details |
| CVE-2024-29967 | In Brocade SANnav before Brocade SANnav v2.31 and v2.3.0a, it was observed that Docker instances inside the appliance have insecure mount points, allowing reading and writing access to sensitive files. The vulnerability could allow a sudo privileged user on the host OS to read and write access to these files. | 4.4 | More Details |
| CVE-2024-30799 | An issue in PX4 Autopilot v1.14 and before allows a remote attacker to execute arbitrary code and cause a denial of service via the Breach Return Point function. | 4.4 | More Details |
| CVE-2024-4031 | Unquoted Search Path or Element vulnerability in Logitech MEVO WEBCAM APP on Windows allows Local Execution of Code. | 4.4 | More Details |
| CVE-2024-26846 | In the Linux kernel, the following vulnerability has been resolved: nvme-fc: do not wait in vain when unloading module The module exit path has race between deleting all controllers and freeing 'left over IDs'. To prevent double free a synchronization between nvme_delete_ctrl and ida_destroy has been added by the initial commit. There is some logic around trying to prevent from hanging forever in wait_for_completion, though it does not handling all cases. E.g. blktests is able to reproduce the situation where the module unload hangs forever. If we completely rely on the cleanup code executed from the nvme_delete_ctrl path, all IDs will be freed eventually. This makes calling ida_destroy unnecessary. We only have to ensure that all nvme_delete_ctrl code has been executed before we leave nvme_fc_exit_module. This is done by flushing the nvme_delete_wq workqueue. While at it, remove the unused nvme_fc_wq workqueue too. | 4.4 | More Details |
| CVE-2024-22813 | An issue in Tormach xsTECH CNC Router, PathPilot Controller v2.9.6 allows attackers to overwrite the hardcoded IP address in the device memory, disrupting network connectivity between the router and the controller. | 4.4 | More Details |
| CVE-2024-3979 | A vulnerability, which was classified as problematic, has been found in COVESA vsomeip up to 3.4.10. Affected by this issue is some unknown functionality. The manipulation leads to race condition. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-261596. | 4.4 | More Details |
| CVE-2023-4509 | It is possible for an API key to be logged in clear text in the audit log file after an invalid login attempt. | 4.3 | More Details |
| CVE-2024-32519 | Missing Authorization vulnerability in GutenGeek GG Woo Feed for WooCommerce.This issue affects GG Woo Feed for WooCommerce: from n/a through 1.2.6. | 4.3 | More Details |
| CVE-2024-32604 | Authorization Bypass Through User-Controlled Key vulnerability in Plechev Andrey WP-Recall.This issue affects WP-Recall: from n/a through 16.26.5. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32516 | Missing Authorization vulnerability in Palscode Multi Currency For WooCommerce.This issue affects Multi Currency For WooCommerce: from n/a through 1.5.5. | 4.3 | More Details |
| CVE-2024-3928 | A vulnerability was found in Dromara open-capacity-platform 2.0.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /actuator/heapdump of the component auth-server. The manipulation leads to information disclosure. 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-261367. | 4.3 | More Details |
| CVE-2024-32517 | Missing Authorization vulnerability in WooCommerce & WordPress Tutorials Custom Thank You Page Customize For WooCommerce by Binary Carpenter.This issue affects Custom Thank You Page Customize For WooCommerce by Binary Carpenter: from n/a through 1.4.12. | 4.3 | More Details |
| CVE-2024-22329 | IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 are vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker could exploit this vulnerability to conduct the SSRF attack. X-Force ID: 279951. | 4.3 | More Details |
| CVE-2024-32333 | TOTOLINK N300RT V2.1.8-B20201030.1539 contains a Store Cross-site scripting (XSS) vulnerability in MAC Filtering under the Firewall Page. | 4.3 | More Details |
| CVE-2024-32520 | Missing Authorization vulnerability in WPClever WPC Grouped Product for WooCommerce.This issue affects WPC Grouped Product for WooCommerce: from n/a through 4.4.2. | 4.3 | More Details |
| CVE-2024-32687 | Missing Authorization vulnerability in WPClever WPC Frequently Bought Together for WooCommerce.This issue affects WPC Frequently Bought Together for WooCommerce: from n/a through 7.0.3. | 4.3 | More Details |
| CVE-2023-6897 | The EAN for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.9.2 via the the 'alg_wc_ean_product_meta' shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to expose potentially sensitive post metadata. | 4.3 | More Details |
| CVE-2024-32689 | Missing Authorization vulnerability in GenialSouls WP Social Comments.This issue affects WP Social Comments: from n/a through 1.7.3. | 4.3 | More Details |
| CVE-2022-34561 | A cross-site scripting (XSS) vulnerability in PHPFox v4.8.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the video description parameter. | 4.3 | More Details |
| CVE-2024-32681 | Missing Authorization vulnerability in BdThemes Prime Slider – Addons For Elementor.This issue affects Prime Slider – Addons For Elementor: from n/a through 3.13.2. | 4.3 | More Details |
| CVE-2024-32522 | Missing Authorization vulnerability in Jaed Mosharraf & Pluginbazar Team Open Close WooCommerce Store.This issue affects Open Close WooCommerce Store: from n/a through 4.9.1. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-0900 | The Elespare – Build Your Blog, News & Magazine Websites with Expert-Designed Template Kits. One Click Import: No Coding Skills Required! plugin for WordPress is vulnerable to unauthorized post creation due to a missing capability check on the elespare_create_post() function hooked via AJAX in all versions up to, and including, 2.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary posts. | 4.3 | More Details |
| CVE-2024-3843 | Insufficient data validation in Downloads in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) | 4.3 | More Details |
| CVE-2024-3932 | A vulnerability classified as problematic has been found in Totara LMS 18.0.1 Build 20231128.01. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261369 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 4.3 | More Details |
| CVE-2024-3844 | Inappropriate implementation in Extensions in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low) | 4.3 | More Details |
| CVE-2024-3845 | Inappropriate implementation in Networks in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to bypass mixed content policy via a crafted HTML page. (Chromium security severity: Low) | 4.3 | More Details |
| CVE-2024-3825 | Versions of the BlazeMeter Jenkins plugin prior to 4.22 contain a flaw which results in credential enumeration | 4.3 | More Details |
| CVE-2024-3664 | The Quick Featured Images plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the set_thumbnail and delete_thumbnail functions in all versions up to, and including, 13.7.0. This makes it possible for authenticated attackers, with contributor-level access and above, to delete thumbnails and add thumbnails to posts they did not author. | 4.3 | More Details |
| CVE-2024-32524 | Missing Authorization vulnerability in Nuggethon Custom Order Statuses for WooCommerce.This issue affects Custom Order Statuses for WooCommerce: from n/a through 1.5.2. | 4.3 | More Details |
| CVE-2024-3846 | Inappropriate implementation in Prompts in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) | 4.3 | More Details |
| CVE-2024-32525 | Missing Authorization vulnerability in Theme My Login.This issue affects Theme My Login: from n/a through 7.1.6. | 4.3 | More Details |
| CVE-2024-32162 | CMSeasy 7.7.7.9 is vulnerable to Arbitrary file deletion. | 4.3 | More Details |
| CVE-2023-41864 | Cross-Site Request Forgery (CSRF) vulnerability in Pepro Dev. Group PeproDev CF7 Database.This issue affects PeproDev CF7 Database: from n/a through 1.8.0. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-29035 | Umbraco is an ASP.NET CMS. Failing webhooks logs are available when solution is not in debug mode. Those logs can contain information that is critical. This vulnerability is fixed in 13.1.1. | 4.1 | More Details |
| CVE-2024-31991 | Mealie is a self hosted recipe manager and meal planner. Prior to 1.4.0, the safe_scrape_html function utilizes a user-controlled URL to issue a request to a remote server. Based on the content of the response, it will either parse the content or disregard it. This function, nor those that call it, add any restrictions on the URL that can be provided, nor is it restricted to being an FQDN (i.e., an IP address can be provided). As this function's return will be handled differently by its caller depending on the response, it is possible for an attacker to use this functionality to positively identify HTTP(s) servers on the local network with any IP/port combination. This issue can result in any authenticated user being able to map HTTP servers on a local network that the Mealie service has access to. Note that by default any user can create an account on a Mealie server, and that the default changeme@example.com user is available with its hard-coded password. This vulnerability is fixed in 1.4.0. | 4.1 | More Details |
| CVE-2023-50007 | Buffer Overflow vulnerability in Ffmpeg v.n6.1-3-g466799d4f5 allows a local attacker to execute arbitrary code via theav_samples_set_silence function in thelibavutil/samplefmt.c:260:9 component. | 4.0 | More Details |
| CVE-2023-48184 | QuickJS before 7414e5f has a quickjs.h JS_FreeValueRT use-after-free because of incorrect garbage collection of async functions with closures. | 3.9 | More Details |
| CVE-2024-30257 | 1Panel is an open source Linux server operation and maintenance management panel. The password verification in the source code uses the != symbol instead hmac.Equal. This may lead to a timing attack vulnerability. This vulnerability is fixed in 1.10.3-lts. | 3.9 | More Details |
| CVE-2024-32314 | Tenda AC500 V2.0.1.9(1307) firmware contains a command injection vulnerablility in the formexeCommand function via the cmdinput parameter. | 3.8 | More Details |
| CVE-2024-4063 | A vulnerability was found in EZVIZ CS-C6-21WFR-8 5.2.7 Build 170628. It has been classified as problematic. This affects an unknown part of the component Davinci Application. The manipulation leads to improper certificate validation. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The identifier VDB-261789 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 3.7 | More Details |
| CVE-2024-4062 | A vulnerability was found in Hualai Xiaofang iSC5 3.2.2_112 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to improper certificate validation. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The identifier of this vulnerability is VDB-261788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 3.7 | More Details |
| CVE-2023-37397 | IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain or modify sensitive information due to improper encryption of certain data. IBM X-Force ID: 259672. | 3.6 | More Details |
| CVE-2023-51796 | Buffer Overflow vulnerability in Ffmpeg v.N113007-g8d24a28d06 allows a local attacker to execute arbitrary code via the libavfilter/f_reverse.c:269:26 in areverse_request_frame. | 3.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-3931 | A vulnerability was found in Totara LMS 18.0.1 Build 20231128.01. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin/roles/check.php of the component Profile Handler. The manipulation of the argument ID Number 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-261368. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 3.5 | More Details |
| CVE-2024-4072 | A vulnerability was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0. It has been classified as problematic. Affected is an unknown function of the file search.php. The manipulation of the argument txtSearch leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-261798 is the identifier assigned to this vulnerability. | 3.5 | More Details |
| CVE-2018-25101 | A vulnerability, which was classified as problematic, has been found in l2c2technologies Koha up to 20180108. This issue affects some unknown processing of the file /cgi-bin/koha/opac-MARCdetail.pl. The manipulation of the argument biblionumber with the input 2"><TEST> leads to cross site scripting. The attack may be initiated remotely. The identifier of the patch is 950fc8e101886821879066b33e389a47fb0a9782. It is recommended to upgrade the affected component. The identifier VDB-261677 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2024-30950 | A stored cross-site scripting (XSS) vulnerability in FUDforum v3.1.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the SQL statements field under /adm/admsql.php. | 3.5 | More Details |
| CVE-2024-4073 | A vulnerability was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file prodList.php. The manipulation of the argument prodType leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-261799. | 3.5 | More Details |
| CVE-2015-10132 | A vulnerability classified as problematic was found in Thimo Grauerholz WP-Spreadplugin up to 3.8.6.1 on WordPress. This vulnerability affects unknown code of the file spreadplugin.php. The manipulation of the argument Spreadplugin leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 3.8.6.6 is able to address this issue. The name of the patch is a9b9afc641854698e80aa5dd9ababfc8e0e57d69. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-261676. | 3.5 | More Details |
| CVE-2024-4074 | A vulnerability was found in Kashipara Online Furniture Shopping Ecommerce Website 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file prodInfo.php. The manipulation of the argument prodId 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-261800. | 3.5 | More Details |
| CVE-2024-4075 | A vulnerability classified as problematic has been found in Kashipara Online Furniture Shopping Ecommerce Website 1.0. This affects an unknown part of the file login.php. The manipulation of the argument txtAddress leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-261801 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2024-30107 | HCL Connections contains a broken access control vulnerability that may expose sensitive information to unauthorized users in certain scenarios. | 3.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-23557 | HCL Connections contains a user enumeration vulnerability. Certain actions could allow an attacker to determine if the user is valid or not, leading to a possible brute force attack. | 3.5 | More Details |
| CVE-2023-38301 | An issue was discovered in a third-party component related to vendor.gsm.serial, shipped on devices from multiple device manufacturers. Various software builds for the BLU View 2, Boost Mobile Celero 5G, Sharp Rouvo V, Motorola Moto G Pure, Motorola Moto G Power, T-Mobile Revvl 6 Pro 5G, and T-Mobile Revvl V+ 5G devices leak the device serial number to a system property that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in these instances they are leaked by a high-privilege process and can be obtained indirectly. The software build fingerprints for each confirmed vulnerable device are as follows: BLU View 2 (BLU/B131DL/B130DL:11/RP1A.200720.011/1672046950:user/release-keys); Boost Mobile Celero 5G (Celero5G/Jupiter/Jupiter:11/RP1A.200720.011/SW_S98119AA1_V067:user/release-keys); Sharp Rouvo V (SHARP/VZW_STTM21VAPP/STTM21VAPP:12/SP1A.210812.016/1KN0_0_530:user/release-keys); Motorola Moto G Pure (motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-2/74844:user/release-keys, motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-7/5cde8:user/release-keys, motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-10/d67faa:user/release-keys, motorola/ellis_trac/ellis:11/RRHS31.Q3-46-110-13/b4a29:user/release-keys, motorola/ellis_trac/ellis:12/S3RH32.20-42-10/1c2540:user/release-keys, motorola/ellis_trac/ellis:12/S3RHS32.20-42-13-2-1/6368dd:user/release-keys, motorola/ellis_a/ellis:11/RRH31.Q3-46-50-2/20fec:user/release-keys, motorola/ellis_vzw/ellis:11/RRH31.Q3-46-138/103bd:user/release-keys, motorola/ellis_vzw/ellis:11/RRHS31.Q3-46-138-2/e5502:user/release-keys, and motorola/ellis_vzw/ellis:12/S3RHS32.20-42-10-14-2/5e0b0:user/release-keys); Motorola Moto G Power (motorola/tonga_g/tonga:11/RRQ31.Q3-68-16-2/e5877:user/release-keys and motorola/tonga_g/tonga:12/S3RQS32.20-42-10-6/f876d3:user/release-keys); T-Mobile Revvl 6 Pro 5G (T-Mobile/Augusta/Augusta:12/SP1A.210812.016/SW_S98121AA1_V070:user/release-keys); and T-Mobile Revvl V+ 5G (T-Mobile/Sprout/Sprout:11/RP1A.200720.011/SW_S98115AA1_V077:user/release-keys). This malicious app reads from the "vendor.gsm.serial" system property to indirectly obtain the device serial number. | 3.4 | More Details |
| CVE-2024-0257 | RoboDK v5.5.4 is vulnerable to heap-based buffer overflow while processing a specific project file. The resulting memory corruption may crash the application. | 3.3 | More Details |
| CVE-2024-26911 | In the Linux kernel, the following vulnerability has been resolved: drm/buddy: Fix alloc_range() error handling code Few users have observed display corruption when they boot the machine to KDE Plasma or playing games. We have root caused the problem that whenever alloc_range() couldn't find the required memory blocks the function was returning SUCCESS in some of the corner cases. The right approach would be if the total allocated size is less than the required size, the function should return -ENOSPC. | 3.3 | More Details |
| CVE-2023-51792 | Buffer Overflow vulnerability in libde265 v1.0.12 allows a local attacker to cause a denial of service via the allocation size exceeding the maximum supported size of 0x10000000000. | 3.3 | More Details |
| CVE-2024-3900 | Out-of-bounds array write in Xpdf 4.05 and earlier, triggered by long Unicode sequence in ActualText. | 2.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-32466 | Tolgee is an open-source localization platform. For the `/v2/projects/translations` and `/v2/projects/{projectId}/translations` endpoints, translation data was returned even when API key was missing `translation.view` scope. However, it was impossible to fetch the data when user was missing this scope. So this is only relevant for API keys generated by users permitted to `translation.view`. This vulnerability is fixed in v3.57.2 | 2.7 | More Details |
| CVE-2024-31040 | Buffer Overflow vulnerability in the get_var_integer function in mqtt_parser.c in NanoMQ 0.21.7 allows remote attackers to cause a denial of service via a series of specially crafted hexstreams. | 2.7 | More Details |
| CVE-2024-29733 | Improper Certificate Validation vulnerability in Apache Airflow FTP Provider. The FTP hook lacks complete certificate validation in FTP_TLS connections, which can potentially be leveraged. Implementing proper certificate validation by passing context=ssl.create_default_context() during FTP_TLS instantiation is used as mitigation to validate the certificates properly. This issue affects Apache Airflow FTP Provider: before 3.7.0. Users are recommended to upgrade to version 3.7.0, which fixes the issue. | 2.7 | More Details |
| CVE-2024-31450 | Owncast is an open source, self-hosted, decentralized, single user live video streaming and chat server. The Owncast application exposes an administrator API at the URL /api/admin. The emoji/delete endpoint of said API allows administrators to delete custom emojis, which are saved on disk. The parameter name is taken from the JSON request and directly appended to the filepath that points to the emoji to delete. By using path traversal sequences (../), attackers with administrative privileges can exploit this endpoint to delete arbitrary files on the system, outside of the emoji directory. This vulnerability is fixed in 0.1.3. | 2.7 | More Details |
| CVE-2024-3177 | A security issue was discovered in Kubernetes where users may be able to launch containers that bypass the mountable secrets policy enforced by the ServiceAccount admission plugin when using containers, init containers, and ephemeral containers with the envFrom field populated. The policy ensures pods running with a service account may only reference secrets specified in the service account's secrets field. Kubernetes clusters are only affected if the ServiceAccount admission plugin and the kubernetes.io/enforce-mountable-secrets annotation are used together with containers, init containers, and ephemeral containers with the envFrom field populated. | 2.7 | More Details |
| CVE-2024-32405 | Cross Site Scripting vulnerability in inducer relate before v.2024.1 allows a remote attacker to escalate privileges via a crafted payload to the Answer field of InlineMultiQuestion parameter on Exam function. | 2.6 | More Details |
| CVE-2023-37396 | IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain sensitive information due to improper encryption of certain data. IBM X-Force ID: 259671. | 2.5 | More Details |
| CVE-2024-32325 | TOTOLINK EX200 V4.0.3c.7646_B20201211 contains a Cross-site scripting (XSS) vulnerability through the ssid parameter in the setWiFiExtenderConfig function. | 2.4 | More Details |
| CVE-2024-32482 | The Tillitis TKey signer device application is an ed25519 signing tool. A vulnerability has been found that makes it possible to disclose portions of the TKey's data in RAM over the USB interface. To exploit the vulnerability an attacker needs to use a custom client application and to touch the TKey. No secret is disclosed. All client applications integrating tkey-device-signer should upgrade to version 1.0.0 to receive a fix. No known workarounds are available. | 2.2 | More Details |
| CVE-2024-29963 | Brocade SANnav OVA before v2.3.1, and v2.3.0a, contain hardcoded TLS keys used by Docker. Note: Brocade SANnav doesn't have access to remote Docker registries. | 1.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26871 | In the Linux kernel, the following vulnerability has been resolved: f2fs: fix NULL pointer dereference in f2fs_submit_page_write() BUG: kernel NULL pointer dereference, address: 0000000000000014 RIP: 0010:f2fs_submit_page_write+0x6cf/0x780 [f2fs] Call Trace: <TASK> ? show_regs+0x6e/0x80 ? __die+0x29/0x70 ? page_fault_oops+0x154/0x4a0 ? prb_read_valid+0x20/0x30 ? __irq_work_queue_local+0x39/0xd0 ? irq_work_queue+0x36/0x70 ? do_user_addr_fault+0x314/0x6c0 ? exc_page_fault+0x7d/0x190 ? asm_exc_page_fault+0x2b/0x30 ? f2fs_submit_page_write+0x6cf/0x780 [f2fs] ? f2fs_submit_page_write+0x736/0x780 [f2fs] do_write_page+0x50/0x170 [f2fs] f2fs_outplace_write_data+0x61/0xb0 [f2fs] f2fs_do_write_data_page+0x3f8/0x660 [f2fs] f2fs_write_single_data_page+0x5bb/0x7a0 [f2fs] f2fs_write_cache_pages+0x3da/0xbe0 [f2fs] ... It is possible that other threads have added this fio to io->bio and submitted the io->bio before entering f2fs_submit_page_write(). At this point io->bio = NULL. If is_end_zone_blkaddr(sbi, fio->new_blkaddr) of this fio is true, then an NULL pointer dereference error occurs at bio_get(io->bio). The original code for determining zone end was after "out:", which would have missed some fio who is zone end. I've moved this code before "skip:" to make sure it's done for each fio. | N/A | More Details |
| CVE-2024-26870 | In the Linux kernel, the following vulnerability has been resolved: NFSv4.2: fix nfs4_listxattr kernel BUG at mm/usercopy.c:102 A call to listxattr() with a buffer size = 0 returns the actual size of the buffer needed for a subsequent call. When size > 0, nfs4_listxattr() does not return an error because either generic_listxattr() or nfs4_listxattr_nfs4_label() consumes exactly all the bytes then size is 0 when calling nfs4_listxattr_nfs4_user() which then triggers the following kernel BUG: [ 99.403778] kernel BUG at mm/usercopy.c:102! [ 99.404063] Internal error: Oops - BUG: 00000000f2000800 [#1] SMP [ 99.408463] CPU: 0 PID: 3310 Comm: python3 Not tainted 6.6.0-61.fc40.aarch64 #1 [ 99.415827] Call trace: [ 99.415985] usercopy_abort+0x70/0xa0 [ 99.416227] __check_heap_object+0x134/0x158 [ 99.416505] check_heap_object+0x150/0x188 [ 99.416696] __check_object_size.part.0+0x78/0x168 [ 99.416886] __check_object_size+0x28/0x40 [ 99.417078] listxattr+0x8c/0x120 [ 99.417252] path_listxattr+0x78/0xe0 [ 99.417476] __arm64_sys_listxattr+0x28/0x40 [ 99.417723] invoke_syscall+0x78/0x100 [ 99.417929] el0_svc_common.constprop.0+0x48/0xf0 [ 99.418186] do_el0_svc+0x24/0x38 [ 99.418376] el0_svc+0x3c/0x110 [ 99.418554] el0t_64_sync_handler+0x120/0x130 [ 99.418788] el0t_64_sync+0x194/0x198 [ 99.418994] Code: aa0003e3 d000a3e0 91310000 97f49bdb (d4210000) Issue is reproduced when generic_listxattr() returns 'system.nfs4_acl', thus calling lisxattr() with size = 16 will trigger the bug. Add check on nfs4_listxattr() to return ERANGE error when it is called with size > 0 and the return value is greater than size. | N/A | More Details |
| CVE-2024-26887 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: Fix memory leak This checks if CONFIG_DEV_COREDUMP is enabled before attempting to clone the skb and also make sure btmtk_process_coredump frees the skb passed following the same logic. | N/A | More Details |
| CVE-2024-26872 | In the Linux kernel, the following vulnerability has been resolved: RDMA/srpt: Do not register event handler until srpt device is fully setup Upon rare occasions, KASAN reports a use-after-free Write in srpt_refresh_port(). This seems to be because an event handler is registered before the srpt device is fully setup and a race condition upon error may leave a partially setup event handler in place. Instead, only register the event handler after srpt device initialization is complete. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26868 | In the Linux kernel, the following vulnerability has been resolved: nfs: fix panic when nfs4_ff_layout_prepare_ds() fails We've been seeing the following panic in production BUG: kernel NULL pointer dereference, address: 0000000000000065 PGD 2f485f067 P4D 2f485f067 PUD 2cc5d8067 PMD 0 RIP: 0010:ff_layout_cancel_io+0x3a/0x90 [nfs_layout_flexfiles] Call Trace: <TASK> ? __die+0x78/0xc0 ? page_fault_oops+0x286/0x380 ? __rpc_execute+0x2c3/0x470 [sunrpc] ? rpc_new_task+0x42/0x1c0 [sunrpc] ? exc_page_fault+0x5d/0x110 ? asm_exc_page_fault+0x22/0x30 ? ff_layout_free_layoutreturn+0x110/0x110 [nfs_layout_flexfiles] ? ff_layout_cancel_io+0x3a/0x90 [nfs_layout_flexfiles] ? ff_layout_cancel_io+0x6f/0x90 [nfs_layout_flexfiles] pnfs_mark_matching_lsegs_return+0x1b0/0x360 [nfsv4] pnfs_error_mark_layout_for_return+0x9e/0x110 [nfsv4] ? ff_layout_send_layouterror+0x50/0x160 [nfs_layout_flexfiles] nfs4_ff_layout_prepare_ds+0x11f/0x290 [nfs_layout_flexfiles] ff_layout_pg_init_write+0xf0/0x1f0 [nfs_layout_flexfiles] __nfs_pageio_add_request+0x154/0x6c0 [nfs] nfs_pageio_add_request+0x26b/0x380 [nfs] nfs_do_writepage+0x111/0x1e0 [nfs] nfs_writepages_callback+0xf/0x30 [nfs] write_cache_pages+0x17f/0x380 ? nfs_pageio_init_write+0x50/0x50 [nfs] ? nfs_writepages+0x6d/0x210 [nfs] ? nfs_writepages+0x6d/0x210 [nfs] nfs_writepages+0x125/0x210 [nfs] do_writepages+0x67/0x220 ? generic_perform_write+0x14b/0x210 filemap_fdatawrite_wbc+0x5b/0x80 file_write_and_wait_range+0x6d/0xc0 nfs_file_fsync+0x81/0x170 [nfs] ? nfs_file_mmap+0x60/0x60 [nfs] __x64_sys_fsync+0x53/0x90 do_syscall_64+0x3d/0x90 entry_SYSCALL_64_after_hwframe+0x46/0xb0 Inspecting the core with drgn I was able to pull this >>> prog.crashed_thread().stack_trace()[0] #0 at 0xffffffffa079657a (ff_layout_cancel_io+0x3a/0x84) in ff_layout_cancel_io at fs/nfs/flexfilelayout/flexfilelayout.c:2021:27 >>> prog.crashed_thread().stack_trace()[0]['idx'] (u32)1 >>> prog.crashed_thread().stack_trace()[0]['flseg'].mirror_array[1].mirror_ds (struct nfs4_ff_layout_ds *)0xffffffffffffffed This is clear from the stack trace, we call nfs4_ff_layout_prepare_ds() which could error out initializing the mirror_ds, and then we go to clean it all up and our check is only for if (!mirror->mirror_ds). This is inconsistent with the rest of the users of mirror_ds, which have if (IS_ERR_OR_NULL(mirror_ds)) to keep from tripping over this exact scenario. Fix this up in ff_layout_cancel_io() to make sure we don't panic when we get an error. I also spot checked all the other instances of checking mirror_ds and we appear to be doing the correct checks everywhere, only unconditionally dereferencing mirror_ds when we know it would be valid. | N/A | More Details |
| CVE-2024-26922 | In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate the parameters of bo mapping operations more clearly Verify the parameters of amdgpu_vm_bo_(map/replace_map/clearing_mappings) in one common place. | N/A | More Details |
| CVE-2024-31869 | Airflow versions 2.7.0 through 2.8.4 have a vulnerability that allows an authenticated user to see sensitive provider configuration via the "configuration" UI page when "non-sensitive-only" was set as "webserver.expose_config" configuration (The celery provider is the only community provider currently that has sensitive configurations). You should migrate to Airflow 2.9 or change your "expose_config" configuration to False as a workaround. This is similar, but different to CVE-2023-46288 https://github.com/advisories/GHSA-9qqg-mh7c-chfq which concerned API, not UI configuration page. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26873 | In the Linux kernel, the following vulnerability has been resolved: scsi: hisi_sas: Fix a deadlock issue related to automatic dump If we issue a disabling PHY command, the device attached with it will go offline, if a 2 bit ECC error occurs at the same time, a hung task may be found: [ 4613.652388] INFO: task kworker/u256:0:165233 blocked for more than 120 seconds. [ 4613.666297] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. [ 4613.674809] task:kworker/u256:0 state:D stack: 0 pid:165233 ppid: 2 flags:0x00000208 [ 4613.683959] Workqueue: 0000:74:02.0_disco_q sas_revalidate_domain [libsas] [ 4613.691518] Call trace: [ 4613.694678] __switch_to+0xf8/0x17c [ 4613.698872] __schedule+0x660/0xee0 [ 4613.703063] schedule+0xac/0x240 [ 4613.706994] schedule_timeout+0x500/0x610 [ 4613.711705] __down+0x128/0x36c [ 4613.715548] down+0x240/0x2d0 [ 4613.719221] hisi_sas_internal_abort_timeout+0x1bc/0x260 [hisi_sas_main] [ 4613.726618] sas_execute_internal_abort+0x144/0x310 [libsas] [ 4613.732976] sas_execute_internal_abort_dev+0x44/0x60 [libsas] [ 4613.739504] hisi_sas_internal_task_abort_dev.isra.0+0xbc/0x1b0 [hisi_sas_main] [ 4613.747499] hisi_sas_dev_gone+0x174/0x250 [hisi_sas_main] [ 4613.753682] sas_notify_lldd_dev_gone+0xec/0x2e0 [libsas] [ 4613.759781] sas_unregister_common_dev+0x4c/0x7a0 [libsas] [ 4613.765962] sas_destruct_devices+0xb8/0x120 [libsas] [ 4613.771709] sas_do_revalidate_domain.constprop.0+0x1b8/0x31c [libsas] [ 4613.778930] sas_revalidate_domain+0x60/0xa4 [libsas] [ 4613.784716] process_one_work+0x248/0x950 [ 4613.789424] worker_thread+0x318/0x934 [ 4613.793878] kthread+0x190/0x200 [ 4613.797810] ret_from_fork+0x10/0x18 [ 4613.802121] INFO: task kworker/u256:4:316722 blocked for more than 120 seconds. [ 4613.816026] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. [ 4613.824538] task:kworker/u256:4 state:D stack: 0 pid:316722 ppid: 2 flags:0x00000208 [ 4613.833670] Workqueue: 0000:74:02.0 hisi_sas_rst_work_handler [hisi_sas_main] [ 4613.841491] Call trace: [ 4613.844647] __switch_to+0xf8/0x17c [ 4613.848852] __schedule+0x660/0xee0 [ 4613.853052] schedule+0xac/0x240 [ 4613.856984] schedule_timeout+0x500/0x610 [ 4613.861695] __down+0x128/0x36c [ 4613.865542] down+0x240/0x2d0 [ 4613.869216] hisi_sas_controller_prereset+0x58/0x1fc [hisi_sas_main] [ 4613.876324] hisi_sas_rst_work_handler+0x40/0x8c [hisi_sas_main] [ 4613.883019] process_one_work+0x248/0x950 [ 4613.887732] worker_thread+0x318/0x934 [ 4613.892204] kthread+0x190/0x200 [ 4613.896118] ret_from_fork+0x10/0x18 [ 4613.900423] INFO: task kworker/u256:1:348985 blocked for more than 121 seconds. [ 4613.914341] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. [ 4613.922852] task:kworker/u256:1 state:D stack: 0 pid:348985 ppid: 2 flags:0x00000208 [ 4613.931984] Workqueue: 0000:74:02.0_event_q sas_port_event_worker [libsas] [ 4613.939549] Call trace: [ 4613.942702] __switch_to+0xf8/0x17c [ 4613.946892] __schedule+0x660/0xee0 [ 4613.951083] schedule+0xac/0x240 [ 4613.955015] schedule_timeout+0x500/0x610 [ 4613.959725] wait_for_common+0x200/0x610 [ 4613.964349] wait_for_completion+0x3c/0x5c [ 4613.969146] flush_workqueue+0x198/0x790 [ 4613.973776] sas_porte_broadcast_rcvd+0x1e8/0x320 [libsas] [ 4613.979960] sas_port_event_worker+0x54/0xa0 [libsas] [ 4613.985708] process_one_work+0x248/0x950 [ 4613.990420] worker_thread+0x318/0x934 [ 4613.994868] kthread+0x190/0x200 [ 4613.998800] ret_from_fork+0x10/0x18 This is because when the device goes offline, we obtain the hisi_hba semaphore and send the ABORT_DEV command to the device. However, the internal abort timed out due to the 2 bit ECC error and triggers automatic dump. In addition, since the hisi_hba semaphore has been obtained, the dump cannot be executed and the controller cannot be reset. Therefore, the deadlocks occur on the following circular dependencies ---truncated--- | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26869 | In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to truncate meta inode pages forcely Below race case can cause data corruption: Thread A GC thread - gc_data_segment - ra_data_block - locked meta_inode page - f2fs_inplace_write_data - invalidate_mapping_pages : fail to invalidate meta_inode page due to lock failure or dirtylwriteback status - f2fs_submit_page_bio : write last dirty data to old blkaddr - move_data_block - load old data from meta_inode page - f2fs_submit_page_write : write old data to new blkaddr Because invalidate_mapping_pages() will skip invalidating page which has unclear status including locked, dirty, writeback and so on, so we need to use truncate_inode_pages_range() instead of invalidate_mapping_pages() to make sure meta_inode page will be dropped. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26867 | In the Linux kernel, the following vulnerability has been resolved: comedi: comedi_8255: Correct error in subdevice initialization The refactoring done in commit 5c57b1ccecc7 ("comedi: comedi_8255: Rework subdevice initialization functions") to the initialization of the io field of struct subdev_8255_private broke all cards using the drivers/comedi/drivers/comedi_8255.c module. Prior to 5c57b1ccecc7, __subdev_8255_init() initialized the io field in the newly allocated struct subdev_8255_private to the non-NULL callback given to the function, otherwise it used a flag parameter to select between subdev_8255_mmio and subdev_8255_io. The refactoring removed that logic and the flag, as subdev_8255_mm_init() and subdev_8255_io_init() now explicitly pass subdev_8255_mmio and subdev_8255_io respectively to __subdev_8255_init(), only __subdev_8255_init() never sets spriv->io to the supplied callback. That spriv->io is NULL leads to a later BUG: BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: 0010 [#1] SMP PTI CPU: 1 PID: 1210 Comm: systemd-udevd Not tainted 6.7.3-x86_64 #1 Hardware name: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX RIP: 0010:0x0 Code: Unable to access opcode bytes at 0xffffffffffffffd6. RSP: 0018:ffffa3f1c02d7b78 EFLAGS: 00010202 RAX: 0000000000000000 RBX: ffff91f847aefd00 RCX: 000000000000009b RDX: 0000000000000003 RSI: 0000000000000001 RDI: ffff91f840f6fc00 RBP: ffff91f840f6fc00 R08: 0000000000000000 R09: 0000000000000001 R10: 0000000000000000 R11: 000000000000005f R12: 0000000000000000 R13: 0000000000000000 R14: ffffffffc0102498 R15: ffff91f847ce6ba8 FS: 00007f72f4e8f500(0000) GS:ffff91f8d5c80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffffffffd6 CR3: 000000010540e000 CR4: 0000000000406f0 Call Trace: <TASK> ? __die_body+0x15/0x57 ? page_fault_oops+0x2ef/0x33c ? insert_vmap_area.constprop.0+0xb6/0xd5 ? alloc_vmap_area+0x529/0x5ee ? exc_page_fault+0x15a/0x489 ? asm_exc_page_fault+0x22/0x30 __subdev_8255_init+0x79/0x8d [comedi_8255] pci_8255_auto_attach+0x11a/0x139 [8255_pci] comedi_auto_config+0xac/0x117 [comedi] ? __pfx___driver_attach+0x10/0x10 pci_device_probe+0x88/0xf9 really_probe+0x101/0x248 __driver_probe_device+0xbb/0xed driver_probe_device+0x1a/0x72 __driver_attach+0xd4/0xed bus_for_each_dev+0x76/0xb8 bus_add_driver+0xbe/0x1be driver_register+0x9a/0xd8 comedi_pci_driver_register+0x28/0x48 [comedi_pci] ? __pfx_pci_8255_driver_init+0x10/0x10 [8255_pci] do_one_initcall+0x72/0x183 do_init_module+0x5b/0x1e8 init_module_from_file+0x86/0xac __do_sys_finit_module+0x151/0x218 do_syscall_64+0x72/0xdb entry_SYSCALL_64_after_hwframe+0x6e/0x76 RIP: 0033:0x7f72f50a0cb9 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 47 71 0c 00 f7 d8 64 89 01 48 RSP: 002b:00007ffd47e512d8 EFLAGS: 00000246 ORIG_RAX: 0000000000000139 RAX: ffffffffffffffda RBX: 0000562dd06ae070 RCX: 00007f72f50a0cb9 RDX: 0000000000000000 RSI: 00007f72f52d32df RDI: 000000000000000e RBP: 0000000000000000 R08: 00007f72f5168b20 R09: 0000000000000000 R10: 0000000000000050 R11: 0000000000000246 R12: 00007f72f52d32df R13: 0000000000020000 R14: 0000562dd06785c0 R15: 0000562dcfd0e9a8 </TASK> Modules linked in: 8255_pci(+) comedi_8255 comedi_pci comedi intel_gtt e100(+) acpi_cpufreq rtc_cmos usbhid CR2: 0000000000000000 ---[ end trace 0000000000000000 ]--- RIP: 0010:0x0 Code: Unable to access opcode bytes at 0xffffffffffffffd6. RSP: 0018:ffffa3f1c02d7b78 EFLAGS: 00010202 RAX: 0000000000000000 RBX: ffff91f847aefd00 RCX: 000000000000009b RDX: 0000000000000003 RSI: 0000000000000001 RDI: ffff91f840f6fc00 RBP: ffff91f840f6fc00 R08: 0000000000000000 R09: 0000000000000001 R10: 0000000000000000 R11: 000000000000005f R12: 0000000000000000 R13: 0000000000000000 R14: ffffffffc0102498 R15: ffff91f847ce6ba8 FS: ---truncated--- | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-23529 | 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-2024-26862 | In the Linux kernel, the following vulnerability has been resolved: packet: annotate data-races around ignore_outgoing ignore_outgoing is read locklessly from dev_queue_xmit_nit() and packet_getsockopt() Add appropriate READ_ONCE()/WRITE_ONCE() annotations. syzbot reported: BUG: KCSAN: data-race in dev_queue_xmit_nit / packet_setsockopt write to 0xffff888107804542 of 1 bytes by task 22618 on cpu 0: packet_setsockopt+0xd83/0xfd0 net/packet/af_packet.c:4003 do_sock_setsockopt net/socket.c:2311 [inline] __sys_setsockopt+0x1d8/0x250 net/socket.c:2334 __do_sys_setsockopt net/socket.c:2343 [inline] __se_sys_setsockopt net/socket.c:2340 [inline] __x64_sys_setsockopt+0x66/0x80 net/socket.c:2340 do_syscall_64+0xd3/0x1d0 entry_SYSCALL_64_after_hwframe+0x6d/0x75 read to 0xffff888107804542 of 1 bytes by task 27 on cpu 1: dev_queue_xmit_nit+0x82/0x620 net/core/dev.c:2248 xmit_one net/core/dev.c:3527 [inline] dev_hard_start_xmit+0xcc/0x3f0 net/core/dev.c:3547 __dev_queue_xmit+0xf24/0x1dd0 net/core/dev.c:4335 dev_queue_xmit include/linux/netdevice.h:3091 [inline] batadv_send_skb_packet+0x264/0x300 net/batman-adv/send.c:108 batadv_send_broadcast_skb+0x24/0x30 net/batman-adv/send.c:127 batadv_iv_ogm_send_to_if net/batman-adv/bat_iv_ogm.c:392 [inline] batadv_iv_ogm_emit net/batman-adv/bat_iv_ogm.c:420 [inline] batadv_iv_send_outstanding_bat_ogm_packet+0x3f0/0x4b0 net/batman-adv/bat_iv_ogm.c:1700 process_one_work kernel/workqueue.c:3254 [inline] process_scheduled_works+0x465/0x990 kernel/workqueue.c:3335 worker_thread+0x526/0x730 kernel/workqueue.c:3416 kthread+0x1d1/0x210 kernel/kthread.c:388 ret_from_fork+0x4b/0x60 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:243 value changed: 0x00 -> 0x01 Reported by Kernel Concurrency Sanitizer on: CPU: 1 PID: 27 Comm: kworker/u8:1 Tainted: G W 6.8.0-syzkaller-08073-g480e035fc4c7 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 02/29/2024 Workqueue: bat_events batadv_iv_send_outstanding_bat_ogm_packet | N/A | More Details |
| CVE-2024-23530 | 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-2024-31745 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-2002. Reason: This candidate is a duplicate of CVE-2024-2002. Notes: All CVE users should reference CVE-2024-2002 instead of this candidate. | N/A | More Details |
| CVE-2024-23528 | 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 Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26866 | In the Linux kernel, the following vulnerability has been resolved: spi: lpspi: Avoid potential use-after-free in probe() fsl_lpspi_probe() is allocating/disposing memory manually with spi_alloc_host()/spi_alloc_target(), but uses devm_spi_register_controller(). In case of error after the latter call the memory will be explicitly freed in the probe function by spi_controller_put() call, but used afterwards by "devm" management outside probe() (spi_unregister_controller() <- devm_spi_unregister() below). Unable to handle kernel NULL pointer dereference at virtual address 0000000000000070 ... Call trace: kernfs_find_ns kernfs_find_and_get_ns sysfs_remove_group sysfs_remove_groups device_remove_attrs device_del spi_unregister_controller devm_spi_unregister release_nodes devres_release_all really_probe driver_probe_device __device_attach_driver bus_for_each_drv __device_attach device_initial_probe bus_probe_device deferred_probe_work_func process_one_work worker_thread kthread ret_from_fork | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26865 | In the Linux kernel, the following vulnerability has been resolved: rds: tcp: Fix use-after-free of net in reqsk_timer_handler(). syzkaller reported a warning of netns tracker [0] followed by KASAN splat [1] and another ref tracker warning [1]. syzkaller could not find a repro, but in the log, the only suspicious sequence was as follows: 18:26:22 executing program 1: r0 = socket$inet6_mptcp(0xa, 0x1, 0x106) ... connect$inet6(r0, &(0x7f0000000080)={0xa, 0x4001, 0x0, @loopback}, 0x1c) (async) The notable thing here is 0x4001 in connect(), which is RDS_TCP_PORT. So, the scenario would be: 1. unshare(CLONE_NEWNET) creates a per netns tcp listener in rds_tcp_listen_init(). 2. syz-executor connect()s to it and creates a reqsk. 3. syz-executor exit()s immediately. 4. netns is dismantled. [0] 5. reqsk timer is fired, and UAF happens while freeing reqsk. [1] 6. listener is freed after RCU grace period. [2] Basically, reqsk assumes that the listener guarantees netns safety until all reqsk timers are expired by holding the listener's refcount. However, this was not the case for kernel sockets. Commit 740ea3c4a0b2 ("tcp: Clean up kernel listener's reqsk in inet_twsk_purge()") fixed this issue only for per-netns ehash. Let's apply the same fix for the global ehash. [0]: ref_tracker: net notrefcnt@0000000065449cc3 has 1/1 users at sk_alloc (./include/net/net_namespace.h:337 net/core/sock.c:2146) inet6_create (net/ipv6/af_inet6.c:192 net/ipv6/af_inet6.c:119) __sock_create (net/socket.c:1572) rds_tcp_listen_init (net/rds/tcp_listen.c:279) rds_tcp_init_net (net/rds/tcp.c:577) ops_init (net/core/net_namespace.c:137) setup_net (net/core/net_namespace.c:340) copy_net_ns (net/core/net_namespace.c:497) create_new_namespaces (kernel/nsproxy.c:110) unshare_nsproxy_namespaces (kernel/nsproxy.c:228 (discriminator 4)) ksys_unshare (kernel/fork.c:3429) __x64_sys_unshare (kernel/fork.c:3496) do_syscall_64 (arch/x86/entry/common.c:52 arch/x86/entry/common.c:83) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:129) ... WARNING: CPU: 0 PID: 27 at lib/ref_tracker.c:179 ref_tracker_dir_exit (lib/ref_tracker.c:179) [1]: BUG: KASAN: slab-use-after-free in inet_csk_reqsk_queue_drop (./include/net/inet_hashtables.h:180 net/ipv4/inet_connection_sock.c:952 net/ipv4/inet_connection_sock.c:966) Read of size 8 at addr ffff88801b370400 by task swapper/0/0 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 Call Trace: <IRQ> dump_stack_lvl (lib/dump_stack.c:107 (discriminator 1)) print_report (mm/kasan/report.c:378 mm/kasan/report.c:488) kasan_report (mm/kasan/report.c:603) inet_csk_reqsk_queue_drop (./include/net/inet_hashtables.h:180 net/ipv4/inet_connection_sock.c:952 net/ipv4/inet_connection_sock.c:966) reqsk_timer_handler (net/ipv4/inet_connection_sock.c:979 net/ipv4/inet_connection_sock.c:1092) call_timer_fn (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:207 ./include/trace/events/timer.h:127 kernel/time/timer.c:1701) __run_timers.part.0 (kernel/time/timer.c:1752 kernel/time/timer.c:2038) run_timer_softirq (kernel/time/timer.c:2053) __do_softirq (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:207 ./include/trace/events/irq.h:142 kernel/softirq.c:554) irq_exit_rcu (kernel/softirq.c:427 kernel/softirq.c:632 kernel/softirq.c:644) sysvec_apic_timer_interrupt (arch/x86/kernel/apic/apic.c:1076 (discriminator 14)) </IRQ> Allocated by task 258 on cpu 0 at 83.612050s: kasan_save_stack (mm/kasan/common.c:48) kasan_save_track (mm/kasan/common.c:68) __kasan_slab_alloc (mm/kasan/common.c:343) kmem_cache_alloc (mm/slub.c:3813 mm/slub.c:3860 mm/slub.c:3867) copy_net_ns (./include/linux/slab.h:701 net/core/net_namespace.c:421 net/core/net_namespace.c:480) create_new_namespaces (kernel/nsproxy.c:110) unshare_nsproxy_name ---truncated--- | N/A | More Details |
| CVE-2024-23526 | 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 Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26863 | In the Linux kernel, the following vulnerability has been resolved: hsr: Fix uninit-value access in hsr_get_node() KMSAN reported the following uninit-value access issue [1]: ===== BUG: KMSAN: uninit-value in hsr_get_node+0xa2e/0xa40 net/hsr/hsr_framereg.c:246 hsr_get_node+0xa2e/0xa40 net/hsr/hsr_framereg.c:246 fill_frame_info net/hsr/hsr_forward.c:577 [inline] hsr_forward_skb+0xe12/0x30e0 net/hsr/hsr_forward.c:615 hsr_dev_xmit+0x1a1/0x270 net/hsr/hsr_device.c:223 __netdev_start_xmit include/linux/netdevice.h:4940 [inline] netdev_start_xmit include/linux/netdevice.h:4954 [inline] xmit_one net/core/dev.c:3548 [inline] dev_hard_start_xmit+0x247/0xa10 net/core/dev.c:3564 __dev_queue_xmit+0x33b8/0x5130 net/core/dev.c:4349 dev_queue_xmit include/linux/netdevice.h:3134 [inline] packet_xmit+0x9c/0x6b0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3087 [inline] packet_sendmsg+0x8b1d/0x9f30 net/packet/af_packet.c:3119 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] __sys_sendto+0x735/0xa10 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x125/0x1c0 net/socket.c:2199 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x6d/0x140 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] kmem_cache_alloc_node+0x5e9/0xb10 mm/slub.c:3523 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:560 __alloc_skb+0x318/0x740 net/core/skbuff.c:651 alloc_skb include/linux/skbuff.h:1286 [inline] alloc_skb_with_frags+0xc8/0xbd0 net/core/skbuff.c:6334 sock_alloc_send_pskb+0xa80/0xbf0 net/core/sock.c:2787 packet_alloc_skb net/packet/af_packet.c:2936 [inline] packet_snd net/packet/af_packet.c:3030 [inline] packet_sendmsg+0x70e8/0x9f30 net/packet/af_packet.c:3119 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] __sys_sendto+0x735/0xa10 net/socket.c:2191 __do_sys_sendto net/socket.c:2203 [inline] __se_sys_sendto net/socket.c:2199 [inline] __x64_sys_sendto+0x125/0x1c0 net/socket.c:2199 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x6d/0x140 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b CPU: 1 PID: 5033 Comm: syz-executor334 Not tainted 6.7.0-syzkaller-00562-g9f8413c4a66f #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 11/17/2023 ===== If the packet type ID field in the Ethernet header is either ETH_P_PRP or ETH_P_HSR, but it is not followed by an HSR tag, hsr_get_skb_sequence_nr() reads an invalid value as a sequence number. This causes the above issue. This patch fixes the issue by returning NULL if the Ethernet header is not followed by an HSR tag. | N/A | More Details |
| CVE-2024-31580 | PyTorch before v2.2.0 was discovered to contain a heap buffer overflow vulnerability in the component /runtime/vararg_functions.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input. | N/A | More Details |
| CVE-2024-30989 | Cross Site Scripting vulnerability in /edit-client-details.php of phpgurukul Client Management System using PHP & MySQL 1.1 allows attackers to execute arbitrary code via the "cname", "comname", "state" and "city" parameter. | N/A | More Details |
| CVE-2024-22061 | A Heap Overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows a remote unauthenticated attacker to execute arbitrary commands | N/A | More Details |
| CVE-2024-30981 | SQL Injection vulnerability in /edit-computer-detail.php in phpgurukul Cyber Cafe Management System Using PHP & MySQL v1.0 allows attackers to run arbitrary SQL commands via editid in the application URL. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26840 | In the Linux kernel, the following vulnerability has been resolved: cachefiles: fix memory leak in cachefiles_add_cache() The following memory leak was reported after unbinding /dev/cachefiles: ========== unreferenced object 0xffff9b674176e3c0 (size 192): comm "cachefilesd2", pid 680, jiffies 4294881224 hex dump (first 32 bytes): 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc ea38a44b): [<ffffffff8eb8a1a5>] kmem_cache_alloc+0x2d5/0x370 [<ffffffff8e917f86>] prepare_creds+0x26/0x2e0 [<ffffffffc002eeef>] cachefiles_determine_cache_security+0x1f/0x120 [<ffffffffc00243ec>] cachefiles_add_cache+0x13c/0x3a0 [<ffffffffc0025216>] cachefiles_daemon_write+0x146/0x1c0 [<ffffffff8ebc4a3b>] vfs_write+0xcb/0x520 [<ffffffff8ebc5069>] ksys_write+0x69/0xf0 [<ffffffff8f6d4662>] do_syscall_64+0x72/0x140 [<ffffffff8f8000aa>] entry_SYSCALL_64_after_hwframe+0x6e/0x76 ========== Put the reference count of cache_cred in cachefiles_daemon_unbind() to fix the problem. And also put cache_cred in cachefiles_add_cache() error branch to avoid memory leaks. | N/A | More Details |
| CVE-2024-26876 | In the Linux kernel, the following vulnerability has been resolved: drm/bridge: adv7511: fix crash on irq during probe Moved IRQ registration down to end of adv7511_probe(). If an IRQ already is pending during adv7511_probe (before adv7511_cec_init) then cec_received_msg_ts could crash using uninitialized data: Unable to handle kernel read from unreadable memory at virtual address 00000000000003d5 Internal error: Oops: 96000004 [#1] PREEMPT_RT SMP Call trace: cec_received_msg_ts+0x48/0x990 [cec] adv7511_cec_irq_process+0x1cc/0x308 [adv7511] adv7511_irq_process+0xd8/0x120 [adv7511] adv7511_irq_handler+0x1c/0x30 [adv7511] irq_thread_fn+0x30/0xa0 irq_thread+0x14c/0x238 kthread+0x190/0x1a8 | N/A | More Details |
| CVE-2024-23531 | An Integer Overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows an unauthenticated remote attacker to perform denial of service attacks. In certain rare conditions this could also lead to reading content from memory. | N/A | More Details |
| CVE-2024-27976 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-24995 | A Race Condition (TOCTOU) vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-24996 | A Heap overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows an unauthenticated remote attacker to execute arbitrary commands. | N/A | More Details |
| CVE-2024-24997 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-32341 | Multiple cross-site scripting (XSS) vulnerabilities in the Home page of WonderCMS v3.4.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into any of the parameters. | N/A | More Details |
| CVE-2024-24998 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-24999 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-25000 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-27975 | An Use-after-free vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-27537 | 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-2024-27536 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Details |
| CVE-2023-48939 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Details |
| CVE-2023-48938 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Details |
| CVE-2023-47357 | 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-2024-27977 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to delete arbitrary files, thereby leading to Denial-of-Service. | N/A | More Details |
| CVE-2024-26874 | In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Fix a null pointer crash in mtk_drm_crtc_finish_page_flip It's possible that mtk_crtc->event is NULL in mtk_drm_crtc_finish_page_flip(). pending_needs_vblank value is set by mtk_crtc->event, but in mtk_drm_crtc_atomic_flush(), it's is not guarded by the same lock in mtk_drm_finish_page_flip(), thus a race condition happens. Consider the following case: CPU1 CPU2 step 1: mtk_drm_crtc_atomic_begin() mtk_crtc->event is not null, step 1: mtk_drm_crtc_atomic_flush: mtk_drm_crtc_update_config( !!mtk_crtc->event) step 2: mtk_crtc_ddp_irq -> mtk_drm_finish_page_flip: lock mtk_crtc->event set to null, pending_needs_vblank set to false unlock pending_needs_vblank set to true, step 2: mtk_crtc_ddp_irq -> mtk_drm_finish_page_flip called again, pending_needs_vblank is still true //null pointer Instead of guarding the entire mtk_drm_crtc_atomic_flush(), it's more efficient to just check if mtk_crtc->event is null before use. | N/A | More Details |
| CVE-2024-27978 | A Null Pointer Dereference vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows an authenticated remote attacker to perform denial of service attacks. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-27984 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to delete specific type of files and/or cause denial of service. | N/A | More Details |
| CVE-2024-29204 | A Heap Overflow vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows a remote unauthenticated attacker to execute arbitrary commands | N/A | More Details |
| CVE-2024-24992 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-24991 | A Null Pointer Dereference vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows an authenticated remote attacker to perform denial of service attacks. | N/A | More Details |
| CVE-2024-26879 | In the Linux kernel, the following vulnerability has been resolved: clk: meson: Add missing clocks to axg_clk_regmaps Some clocks were missing from axg_clk_regmaps, which caused kernel panic during cat /sys/kernel/debug/clk/clk_summary [ 57.349402] Unable to handle kernel NULL pointer dereference at virtual address 00000000000001fc ... [ 57.430002] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [ 57.436900] pc : regmap_read+0x1c/0x88 [ 57.440608] lr : clk_regmap_gate_is_enabled+0x3c/0xb0 [ 57.445611] sp : ffff800082f1b690 [ 57.448888] x29: ffff800082f1b690 x28: 0000000000000000 x27: ffff800080eb9a70 [ 57.455961] x26: 0000000000000007 x25: 0000000000000016 x24: 0000000000000000 [ 57.463033] x23: ffff800080e8b488 x22: 0000000000000015 x21: ffff00000e7e7000 [ 57.470106] x20: ffff00000400ec00 x19: 0000000000000000 x18: ffffffffffffffff [ 57.477178] x17: 0000000000000000 x16: 0000000000000000 x15: ffff0000042a3000 [ 57.484251] x14: 0000000000000000 x13: ffff0000042a2fec x12: 0000000005f5e100 [ 57.491323] x11: abcc77118461cefd x10: 0000000000000020 x9 : ffff8000805e4b24 [ 57.498396] x8 : ffff0000028063c0 x7 : ffff800082f1b710 x6 : ffff800082f1b710 [ 57.505468] x5 : 00000000ffffffd0 x4 : ffff800082f1b6e0 x3 : 0000000000001000 [ 57.512541] x2 : ffff800082f1b6e4 x1 : 000000000000012c x0 : 0000000000000000 [ 57.519615] Call trace: [ 57.522030] regmap_read+0x1c/0x88 [ 57.525393] clk_regmap_gate_is_enabled+0x3c/0xb0 [ 57.530050] clk_core_is_enabled+0x44/0x120 [ 57.534190] clk_summary_show_subtree+0x154/0x2f0 [ 57.538847] clk_summary_show_subtree+0x220/0x2f0 [ 57.543505] clk_summary_show_subtree+0x220/0x2f0 [ 57.548162] clk_summary_show_subtree+0x220/0x2f0 [ 57.552820] clk_summary_show_subtree+0x220/0x2f0 [ 57.557477] clk_summary_show_subtree+0x220/0x2f0 [ 57.562135] clk_summary_show_subtree+0x220/0x2f0 [ 57.566792] clk_summary_show_subtree+0x220/0x2f0 [ 57.571450] clk_summary_show+0x84/0xb8 [ 57.575245] seq_read_iter+0x1bc/0x4b8 [ 57.578954] seq_read+0x8c/0xd0 [ 57.582059] full_proxy_read+0x68/0xc8 [ 57.585767] vfs_read+0xb0/0x268 [ 57.588959] ksys_read+0x70/0x108 [ 57.592236] __arm64_sys_read+0x24/0x38 [ 57.596031] invoke_syscall+0x50/0x128 [ 57.599740] el0_svc_common.constprop.0+0x48/0xf8 [ 57.604397] do_el0_svc+0x28/0x40 [ 57.607675] el0_svc+0x34/0xb8 [ 57.610694] el0t_64_sync_handler+0x13c/0x158 [ 57.615006] el0t_64_sync+0x190/0x198 [ 57.618635] Code: a9bd7bfd 910003fd a90153f3 aa0003f3 (b941fc00) [ 57.624668] ---[ end trace 0000000000000000 ]--- [jbrunet: add missing Fixes tag] | N/A | More Details |
| CVE-2024-23535 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-23534 | An Unrestricted File-upload vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-23533 | An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an authenticated remote attacker to read sensitive information in memory. | N/A | More Details |
| CVE-2024-26878 | In the Linux kernel, the following vulnerability has been resolved: quota: Fix potential NULL pointer dereference Below race may cause NULL pointer dereference P1 P2 dquot_free_inode quota_off drop_dquot_ref remove_dquot_ref dquots = i_dquot(inode) dquots = i_dquot(inode) srcu_read_lock dquots[cnt]) != NULL (1) dquots[type] = NULL (2) spin_lock(&dquots[cnt]->dq_dqb_lock) (3) .... If dquot_free_inode(or other routines) checks inode's quota pointers (1) before quota_off sets it to NULL(2) and use it (3) after that, NULL pointer dereference will be triggered. So let's fix it by using a temporary pointer to avoid this issue. | N/A | More Details |
| CVE-2024-26877 | In the Linux kernel, the following vulnerability has been resolved: crypto: xilinx - call finalize with bh disabled When calling crypto_finalize_request, BH should be disabled to avoid triggering the following calltrace: ------------[ cut here ]------------ WARNING: CPU: 2 PID: 74 at crypto/crypto_engine.c:58 crypto_finalize_request+0xa0/0x118 Modules linked in: cryptodev(O) CPU: 2 PID: 74 Comm: firmware:zynqmp Tainted: G O 6.8.0-rc1-yocto-standard #323 Hardware name: ZynqMP ZCU102 Rev1.0 (DT) pstate: 40000005 (nZcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : crypto_finalize_request+0xa0/0x118 lr : crypto_finalize_request+0x104/0x118 sp : ffffffc085353ce0 x29: ffffffc085353ce0 x28: 0000000000000000 x27: ffffff8808ea8688 x26: ffffffc081715038 x25: 0000000000000000 x24: ffffff880100db00 x23: ffffff880100da80 x22: 0000000000000000 x21: 0000000000000000 x20: ffffff8805b14000 x19: ffffff880100da80 x18: 0000000000010450 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000003 x13: 0000000000000000 x12: ffffff880100dad0 x11: 0000000000000000 x10: ffffffc0832dcd08 x9 : ffffffc0812416d8 x8 : 00000000000001f4 x7 : ffffffc0830d2830 x6 : 0000000000000001 x5 : ffffffc082091000 x4 : ffffffc082091658 x3 : 0000000000000000 x2 : ffffffc7f9653000 x1 : 0000000000000000 x0 : ffffff8802d20000 Call trace: crypto_finalize_request+0xa0/0x118 crypto_finalize_aead_request+0x18/0x30 zynqmp_handle_aes_req+0xcc/0x388 crypto_pump_work+0x168/0x2d8 kthread_worker_fn+0xfc/0x3a0 kthread+0x118/0x138 ret_from_fork+0x10/0x20 irq event stamp: 40 hardirqs last enabled at (39): [<ffffffc0812416f8>] _raw_spin_unlock_irqrestore+0x70/0xb0 hardirqs last disabled at (40): [<ffffffc08122d208>] el1_dbg+0x28/0x90 softirqs last enabled at (36): [<ffffffc080017dec>] kernel_neon_begin+0x8c/0xf0 softirqs last disabled at (34): [<ffffffc080017dc0>] kernel_neon_begin+0x60/0xf0 ---[ end trace 0000000000000000 ]--- | N/A | More Details |
| CVE-2024-26860 | In the Linux kernel, the following vulnerability has been resolved: dm-integrity: fix a memory leak when rechecking the data Memory for the "checksums" pointer will leak if the data is rechecked after checksum failure (because the associated kfree won't happen due to 'goto skip_io'). Fix this by freeing the checksums memory before recheck, and just use the "checksum_onstack" memory for storing checksum during recheck. | N/A | More Details |
| CVE-2024-23532 | An out-of-bounds Read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows an authenticated remote attacker to perform denial of service attacks. In certain conditions this could also lead to remote code execution. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26861 | In the Linux kernel, the following vulnerability has been resolved: wireguard: receive: annotate data-race around receiving_counter.counter Syzkaller with KCSAN identified a data-race issue when accessing keypair->receiving_counter.counter. Use READ_ONCE() and WRITE_ONCE() annotations to mark the data race as intentional. BUG: KCSAN: data-race in wg_packet_decrypt_worker / wg_packet_rx_poll write to 0xffff888107765888 of 8 bytes by interrupt on cpu 0: counter_validate drivers/net/wireguard/receive.c:321 [inline] wg_packet_rx_poll+0x3ac/0xf00 drivers/net/wireguard/receive.c:461 __napi_poll+0x60/0x3b0 net/core/dev.c:6536 napi_poll net/core/dev.c:6605 [inline] net_rx_action+0x32b/0x750 net/core/dev.c:6738 __do_softirq+0xc4/0x279 kernel/softirq.c:553 do_softirq+0x5e/0x90 kernel/softirq.c:454 __local_bh_enable_ip+0x64/0x70 kernel/softirq.c:381 __raw_spin_unlock_bh include/linux/spinlock_api_smp.h:167 [inline] _raw_spin_unlock_bh+0x36/0x40 kernel/locking/spinlock.c:210 spin_unlock_bh include/linux/spinlock.h:396 [inline] ptr_ring_consume_bh include/linux/ptr_ring.h:367 [inline] wg_packet_decrypt_worker+0x6c5/0x700 drivers/net/wireguard/receive.c:499 process_one_work kernel/workqueue.c:2633 [inline] ... read to 0xffff888107765888 of 8 bytes by task 3196 on cpu 1: decrypt_packet drivers/net/wireguard/receive.c:252 [inline] wg_packet_decrypt_worker+0x220/0x700 drivers/net/wireguard/receive.c:501 process_one_work kernel/workqueue.c:2633 [inline] process_scheduled_works+0x5b8/0xa30 kernel/workqueue.c:2706 worker_thread+0x525/0x730 kernel/workqueue.c:2787 ... | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26891 | In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Don't issue ATS Invalidation request when device is disconnected For those endpoint devices connect to system via hotplug capable ports, users could request a hot reset to the device by flapping device's link through setting the slot's link control register, as pciehp_ist() DLLSC interrupt sequence response, pciehp will unload the device driver and then power it off. thus cause an IOMMU device-TLB invalidation (Intel VT-d spec, or ATS Invalidation in PCIe spec r6.1) request for non-existence target device to be sent and deadly loop to retry that request after ITE fault triggered in interrupt context. That would cause following continuous hard lockup warning and system hang [ 4211.433662] pcieport 0000:17:01.0: pciehp: Slot(108): Link Down [ 4211.433664] pcieport 0000:17:01.0: pciehp: Slot(108): Card not present [ 4223.822591] NMI watchdog: Watchdog detected hard LOCKUP on cpu 144 [ 4223.822622] CPU: 144 PID: 1422 Comm: irq/57-pciehp Kdump: loaded Tainted: G S OE kernel version xxxx [ 4223.822623] Hardware name: vendorname xxxx 666-106, BIOS 01.01.02.03.01 05/15/2023 [ 4223.822623] RIP: 0010:qi_submit_sync+0x2c0/0x490 [ 4223.822624] Code: 48 be 00 00 00 00 00 08 00 00 49 85 74 24 20 0f 95 c1 48 8b 57 10 83 c1 04 83 3c 1a 03 0f 84 a2 01 00 00 49 8b 04 24 8b 70 34 <40> f6 c6 1 0 74 17 49 8b 04 24 8b 80 80 00 00 00 89 c2 d3 fa 41 39 [ 4223.822624] RSP: 0018:ffffc4f074f0bbb8 EFLAGS: 00000093 [ 4223.822625] RAX: ffffc4f040059000 RBX: 0000000000000014 RCX: 0000000000000005 [ 4223.822625] RDX: ffff9f3841315800 RSI: 0000000000000000 RDI: ffff9f38401a8340 [ 4223.822625] RBP: ffff9f38401a8340 R08: ffffc4f074f0bc00 R09: 0000000000000000 [ 4223.822626] R10: 0000000000000010 R11: 0000000000000018 R12: ffff9f384005e200 [ 4223.822626] R13: 0000000000000004 R14: 0000000000000046 R15: 0000000000000004 [ 4223.822626] FS: 0000000000000000(0000) GS:ffffa237ae400000(0000) knlGS:0000000000000000 [ 4223.822627] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [ 4223.822627] CR2: 00007ffe86515d80 CR3: 000002fd3000a001 CR4: 0000000000770ee0 [ 4223.822627] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [ 4223.822628] DR3: 0000000000000000 DR6: 00000000fffe07f0 DR7: 0000000000000400 [ 4223.822628] PKRU: 55555554 [ 4223.822628] Call Trace: [ 4223.822628] qi_flush_dev_iotlb+0xb1/0xd0 [ 4223.822628] __dmar_remove_one_dev_info+0x224/0x250 [ 4223.822629] dmar_remove_one_dev_info+0x3e/0x50 [ 4223.822629] intel_iommu_release_device+0x1f/0x30 [ 4223.822629] iommu_release_device+0x33/0x60 [ 4223.822629] iommu_bus_notifier+0x7f/0x90 [ 4223.822630] blocking_notifier_call_chain+0x60/0x90 [ 4223.822630] device_del+0x2e5/0x420 [ 4223.822630] pci_remove_bus_device+0x70/0x110 [ 4223.822630] pciehp_unconfigure_device+0x7c/0x130 [ 4223.822631] pciehp_disable_slot+0x6b/0x100 [ 4223.822631] pciehp_handle_presence_or_link_change+0xd8/0x320 [ 4223.822631] pciehp_ist+0x176/0x180 [ 4223.822631] ? irq_finalize_oneshot.part.50+0x110/0x110 [ 4223.822632] irq_thread_fn+0x19/0x50 [ 4223.822632] irq_thread+0x104/0x190 [ 4223.822632] ? irq_forced_thread_fn+0x90/0x90 [ 4223.822632] ? irq_thread_check_affinity+0xe0/0xe0 [ 4223.822633] kthread+0x114/0x130 [ 4223.822633] ? __kthread_cancel_work+0x40/0x40 [ 4223.822633] ret_from_fork+0x1f/0x30 [ 4223.822633] Kernel panic - not syncing: Hard LOCKUP [ 4223.822634] CPU: 144 PID: 1422 Comm: irq/57-pciehp Kdump: loaded Tainted: G S OE kernel version xxxx [ 4223.822634] Hardware name: vendorname xxxx 666-106, BIOS 01.01.02.03.01 05/15/2023 [ 4223.822634] Call Trace: [ 4223.822634] <NMI> [ 4223.822635] dump_stack+0x6d/0x88 [ 4223.822635] panic+0x101/0x2d0 [ 4223.822635] ? ret_from_fork+0x11/0x30 [ 4223.822635] nmi_panic.cold.14+0xc/0xc [ 4223.822636] watchdog_overflow_callback.cold.8+0x6d/0x81 [ 4223.822636] __perf_event_overflow+0x4f/0xf0 [ 4223.822636] handle_pmi_common ---truncated--- | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26921 | In the Linux kernel, the following vulnerability has been resolved: inet: inet_defrag: prevent sk release while still in use ip_local_out() and other functions can pass skb->sk as function argument. If the skb is a fragment and reassembly happens before such function call returns, the sk must not be released. This affects skb fragments reassembled via netfilter or similar modules, e.g. openvswitch or ct_act.c, when run as part of tx pipeline. Eric Dumazet made an initial analysis of this bug. Quoting Eric: Calling ip_defrag() in output path is also implying skb_orphan(), which is buggy because output path relies on sk not disappearing. A relevant old patch about the issue was : 8282f27449bf ("inet: frag: Always orphan skbs inside ip_defrag()") [..] net/ipv4/ip_output.c depends on skb->sk being set, and probably to an inet socket, not an arbitrary one. If we orphan the packet in ipvlan, then downstream things like FQ packet scheduler will not work properly. We need to change ip_defrag() to only use skb_orphan() when really needed, ie whenever frag_list is going to be used. Eric suggested to stash sk in fragment queue and made an initial patch. However there is a problem with this: If skb is refragmented again right after, ip_do_fragment() will copy head->sk to the new fragments, and sets up destructor to sock_wfree. IOW, we have no choice but to fix up sk_wmem accouting to reflect the fully reassembled skb, else wmem will underflow. This change moves the orphan down into the core, to last possible moment. As ip_defrag_offset is aliased with sk_buff->sk member, we must move the offset into the FRAG_CB, else skb->sk gets clobbered. This allows to delay the orphaning long enough to learn if the skb has to be queued or if the skb is completing the reasm queue. In the former case, things work as before, skb is orphaned. This is safe because skb gets queued/stolen and won't continue past reasm engine. In the latter case, we will steal the skb->sk reference, reattach it to the head skb, and fix up wmem accouting when inet_frag inflates truesize. | N/A | More Details |
| CVE-2024-26888 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: msft: Fix memory leak Fix leaking buffer allocated to send MSFT_OP_LE_MONITOR_ADVERTISEMENT. | N/A | More Details |
| CVE-2024-26825 | In the Linux kernel, the following vulnerability has been resolved: nfc: nci: free rx_data_reassembly skb on NCI device cleanup rx_data_reassembly skb is stored during NCI data exchange for processing fragmented packets. It is dropped only when the last fragment is processed or when an NTF packet with NCI_OP_RF_DEACTIVATE_NTF opcode is received. However, the NCI device may be deallocated before that which leads to skb leak. As by design the rx_data_reassembly skb is bound to the NCI device and nothing prevents the device to be freed before the skb is processed in some way and cleaned, free it on the NCI device cleanup. Found by Linux Verification Center (linuxtesting.org) with Syzkaller. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26895 | In the Linux kernel, the following vulnerability has been resolved: wifi: wilc1000: prevent use-after-free on vif when cleaning up all interfaces wilc_netdev_cleanup currently triggers a KASAN warning, which can be observed on interface registration error path, or simply by removing the module/unbinding device from driver: echo spi0.1 > /sys/bus/spi/drivers/wilc1000_spi/unbind ================================================================== BUG: KASAN: slab-use-after-free in wilc_netdev_cleanup+0x508/0x5cc Read of size 4 at addr c54d1ce8 by task sh/86 CPU: 0 PID: 86 Comm: sh Not tainted 6.8.0-rc1+ #117 Hardware name: Atmel SAMA5 unwind_backtrace from show_stack+0x18/0x1c show_stack from dump_stack_lvl+0x34/0x58 dump_stack_lvl from print_report+0x154/0x500 print_report from kasan_report+0xac/0xd8 kasan_report from wilc_netdev_cleanup+0x508/0x5cc wilc_netdev_cleanup from wilc_bus_remove+0xc8/0xec wilc_bus_remove from spi_remove+0x8c/0xac spi_remove from device_release_driver_internal+0x434/0x5f8 device_release_driver_internal from unbind_store+0xbc/0x108 unbind_store from kernfs_fop_write_iter+0x398/0x584 kernfs_fop_write_iter from vfs_write+0x728/0xf88 vfs_write from ksys_write+0x110/0x1e4 ksys_write from ret_fast_syscall+0x0/0x1c [...] Allocated by task 1: kasan_save_track+0x30/0x5c __kasan_kmalloc+0x8c/0x94 __kmalloc_node+0x1cc/0x3e4 kvmalloc_node+0x48/0x180 alloc_netdev_mqs+0x68/0x11dc alloc_etherdev_mqs+0x28/0x34 wilc_netdev_ifc_init+0x34/0x8ec wilc_cfg80211_init+0x690/0x910 wilc_bus_probe+0xe0/0x4a0 spi_probe+0x158/0x1b0 really_probe+0x270/0xdf4 __driver_probe_device+0x1dc/0x580 driver_probe_device+0x60/0x140 __driver_attach+0x228/0x5d4 bus_for_each_dev+0x13c/0x1a8 bus_add_driver+0x2a0/0x608 driver_register+0x24c/0x578 do_one_initcall+0x180/0x310 kernel_init_freeable+0x424/0x484 kernel_init+0x20/0x148 ret_from_fork+0x14/0x28 Freed by task 86: kasan_save_track+0x30/0x5c kasan_save_free_info+0x38/0x58 __kasan_slab_free+0xe4/0x140 kfree+0xb0/0x238 device_release+0xc0/0x2a8 kobject_put+0x1d4/0x46c netdev_run_todo+0x8fc/0x11d0 wilc_netdev_cleanup+0x1e4/0x5cc wilc_bus_remove+0xc8/0xec spi_remove+0x8c/0xac device_release_driver_internal+0x434/0x5f8 unbind_store+0xbc/0x108 kernfs_fop_write_iter+0x398/0x584 vfs_write+0x728/0xf88 ksys_write+0x110/0x1e4 ret_fast_syscall+0x0/0x1c [...] David Mosberger-Tan initial investigation [1] showed that this use-after-free is due to netdevice unregistration during vif list traversal. When unregistering a net device, since the needs_free_netdev has been set to true during registration, the netdevice object is also freed, and as a consequence, the corresponding vif object too, since it is attached to it as private netdevice data. The next occurrence of the loop then tries to access freed vif pointer to the list to move forward in the list. Fix this use-after-free thanks to two mechanisms: - navigate in the list with list_for_each_entry_safe, which allows to safely modify the list as we go through each element. For each element, remove it from the list with list_del_rcu - make sure to wait for RCU grace period end after each vif removal to make sure it is safe to free the corresponding vif too (through unregister_netdev) Since we are in a RCU "modifier" path (not a "reader" path), and because such path is expected not to be concurrent to any other modifier (we are using the vif_mutex lock), we do not need to use RCU list API, that's why we can benefit from list_for_each_entry_safe. [1] https://lore.kernel.org/linux-wireless/ab077dbe58b1ea5de0a3b2ca21f275a07af967d2.camel@egauge.net/ | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26826 | In the Linux kernel, the following vulnerability has been resolved: mptcp: fix data re-injection from stale subflow When the MPTCP PM detects that a subflow is stale, all the packet scheduler must re-inject all the mptcp-level unacked data. To avoid acquiring unneeded locks, it first try to check if any unacked data is present at all in the RTX queue, but such check is currently broken, as it uses TCP-specific helper on an MPTCP socket. Funnily enough fuzzers and static checkers are happy, as the accessed memory still belongs to the mptcp_sock struct, and even from a functional perspective the recovery completed successfully, as the short-cut test always failed. A recent unrelated TCP change - commit d5fed5addb2b ("tcp: reorganize tcp_sock fast path variables") - exposed the issue, as the tcp field reorganization makes the mptcp code always skip the re-inection. Fix the issue dropping the bogus call: we are on a slow path, the early optimization proved once again to be evil. | N/A | More Details |
| CVE-2024-26896 | In the Linux kernel, the following vulnerability has been resolved: wifi: wfx: fix memory leak when starting AP Kmemleak reported this error: unreferenced object 0xd73d1180 (size 184): comm "wpa_supplicant", pid 1559, jiffies 13006305 (age 964.245s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 1e 00 01 00 00 00 00 00 ..... backtrace: [<5ca11420>] kmem_cache_alloc+0x20c/0x5ac [<127bdd74>] __alloc_skb+0x144/0x170 [<fb8a5e38>] __netdev_alloc_skb+0x50/0x180 [<0f9fa1d5>] __ieee80211_beacon_get+0x290/0x4d4 [mac80211] [<7accd02d>] ieee80211_beacon_get_tim+0x54/0x18c [mac80211] [<41e25cc3>] wfx_start_ap+0xc8/0x234 [wfx] [<93a70356>] ieee80211_start_ap+0x404/0x6b4 [mac80211] [<a4a661cd>] nl80211_start_ap+0x76c/0x9e0 [cfg80211] [<47bd8b68>] genl_rcv_msg+0x198/0x378 [<453ef796>] netlink_rcv_skb+0xd0/0x130 [<6b7c977a>] genl_rcv+0x34/0x44 [<66b2d04d>] netlink_unicast+0x1b4/0x258 [<f965b9b6>] netlink_sendmsg+0x1e8/0x428 [<aadb8231>] ____sys_sendmsg+0x1e0/0x274 [<d2b5212d>] ___sys_sendmsg+0x80/0xb4 [<69954f45>] __sys_sendmsg+0x64/0xa8 unreferenced object 0xce087000 (size 1024): comm "wpa_supplicant", pid 1559, jiffies 13006305 (age 964.246s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 10 00 07 40 00 00 00 00 00 00 00 00 00 00 00 00 ...@..... backtrace: [<9a993714>] __kmalloc_track_caller+0x230/0x600 [<f83ea192>] kmalloc_reserve.constprop.0+0x30/0x74 [<a2c61343>] __alloc_skb+0xa0/0x170 [<fb8a5e38>] __netdev_alloc_skb+0x50/0x180 [<0f9fa1d5>] __ieee80211_beacon_get+0x290/0x4d4 [mac80211] [<7accd02d>] ieee80211_beacon_get_tim+0x54/0x18c [mac80211] [<41e25cc3>] wfx_start_ap+0xc8/0x234 [wfx] [<93a70356>] ieee80211_start_ap+0x404/0x6b4 [mac80211] [<a4a661cd>] nl80211_start_ap+0x76c/0x9e0 [cfg80211] [<47bd8b68>] genl_rcv_msg+0x198/0x378 [<453ef796>] netlink_rcv_skb+0xd0/0x130 [<6b7c977a>] genl_rcv+0x34/0x44 [<66b2d04d>] netlink_unicast+0x1b4/0x258 [<f965b9b6>] netlink_sendmsg+0x1e8/0x428 [<aadb8231>] ____sys_sendmsg+0x1e0/0x274 [<d2b5212d>] ___sys_sendmsg+0x80/0xb4 However, since the kernel is build optimized, it seems the stack is not accurate. It appears the issue is related to wfx_set_mfp_ap(). The issue is obvious in this function: memory allocated by ieee80211_beacon_get() is never released. Fixing this leak makes kmemleak happy. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26897 | In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: delay all of ath9k_wmi_event_tasklet() until init is complete The ath9k_wmi_event_tasklet() used in ath9k_htc assumes that all the data structures have been fully initialised by the time it runs. However, because of the order in which things are initialised, this is not guaranteed to be the case, because the device is exposed to the USB subsystem before the ath9k driver initialisation is completed. We already committed a partial fix for this in commit: 8b3046abc99e ("ath9k_htc: fix NULL pointer dereference at ath9k_htc_tx_get_packet()") However, that commit only aborted the WMI_TXSTATUS_EVENTID command in the event tasklet, pairing it with an "initialisation complete" bit in the TX struct. It seems syzbot managed to trigger the race for one of the other commands as well, so let's just move the existing synchronisation bit to cover the whole tasklet (setting it at the end of ath9k_htc_probe_device() instead of inside ath9k_tx_init()). | N/A | More Details |
| CVE-2024-1681 | corydolphin/flask-cors is vulnerable to log injection when the log level is set to debug. An attacker can inject fake log entries into the log file by sending a specially crafted GET request containing a CRLF sequence in the request path. This vulnerability allows attackers to corrupt log files, potentially covering tracks of other attacks, confusing log post-processing tools, and forging log entries. The issue is due to improper output neutralization for logs. | N/A | More Details |
| CVE-2024-26827 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |
| CVE-2024-26829 | In the Linux kernel, the following vulnerability has been resolved: media: ir_toy: fix a memleak in irtoy_tx When irtoy_command fails, buf should be freed since it is allocated by irtoy_tx, or there is a memleak. | N/A | More Details |
| CVE-2024-26830 | In the Linux kernel, the following vulnerability has been resolved: i40e: Do not allow untrusted VF to remove administratively set MAC Currently when PF administratively sets VF's MAC address and the VF is put down (VF tries to delete all MACs) then the MAC is removed from MAC filters and primary VF MAC is zeroed. Do not allow untrusted VF to remove primary MAC when it was set administratively by PF. Reproducer: 1) Create VF 2) Set VF interface up 3) Administratively set the VF's MAC 4) Put VF interface down [root@host ~]# echo 1 > /sys/class/net/enp2s0f0/device/sriov_numvfs [root@host ~]# ip link set enp2s0f0v0 up [root@host ~]# ip link set enp2s0f0 vf 0 mac fe:6c:b5:da:c7:7d [root@host ~]# ip link show enp2s0f0 23: enp2s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000 link/ether 3c:ec:ef:b7:dd:04 brd ff:ff:ff:ff:ff:ff vf 0 link/ether fe:6c:b5:da:c7:7d brd ff:ff:ff:ff:ff:ff, spoof checking on, link-state auto, trust off [root@host ~]# ip link set enp2s0f0v0 down [root@host ~]# ip link show enp2s0f0 23: enp2s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000 link/ether 3c:ec:ef:b7:dd:04 brd ff:ff:ff:ff:ff:ff vf 0 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking on, link-state auto, trust off | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26831 | In the Linux kernel, the following vulnerability has been resolved: net/handshake: Fix handshake_req_destroy_test1 Recently, handshake_req_destroy_test1 started failing: Expected handshake_req_destroy_test == req, but handshake_req_destroy_test == 0000000000000000 req == 0000000060f99b40 not ok 11 req_destroy works This is because "sock_release(sock)" was replaced with "fput(filp)" to address a memory leak. Note that sock_release() is synchronous but fput() usually delays the final close and clean-up. The delay is not consequential in the other cases that were changed but handshake_req_destroy_test1 is testing that handshake_req_cancel() followed by closing the file actually does call the ->hp_destroy method. Thus the PTR_EQ test at the end has to be sure that the final close is complete before it checks the pointer. We cannot use a completion here because if ->hp_destroy is never called (ie, there is an API bug) then the test will hang. Reported by: Guenter Roeck <linux@roeck-us.net> | N/A | More Details |
| CVE-2024-26904 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |
| CVE-2024-26832 | In the Linux kernel, the following vulnerability has been resolved: mm: zswap: fix missing folio cleanup in writeback race path In zswap_writeback_entry(), after we get a folio from __read_swap_cache_async(), we grab the tree lock again to check that the swap entry was not invalidated and recycled. If it was, we delete the folio we just added to the swap cache and exit. However, __read_swap_cache_async() returns the folio locked when it is newly allocated, which is always true for this path, and the folio is ref'd. Make sure to unlock and put the folio before returning. This was discovered by code inspection, probably because this path handles a race condition that should not happen often, and the bug would not crash the system, it will only strand the folio indefinitely. | N/A | More Details |
| CVE-2024-26905 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |
| CVE-2024-26845 | In the Linux kernel, the following vulnerability has been resolved: scsi: target: core: Add TMF to tmr_list handling An abort that is responded to by iSCSI itself is added to tmr_list but does not go to target core. A LUN_RESET that goes through tmr_list takes a refcounter on the abort and waits for completion. However, the abort will be never complete because it was not started in target core. Unable to locate ITT: 0x05000000 on CID: 0 Unable to locate RefTaskTag: 0x05000000 on CID: 0. wait_for_tasks: Stopping tmf LUN_RESET with tag 0x0 ref_task_tag 0x0 i_state 34 t_state ISTATE_PROCESSING refcnt 2 transport_state active,stop,fabric_stop wait for tasks: tmf LUN_RESET with tag 0x0 ref_task_tag 0x0 i_state 34 t_state ISTATE_PROCESSING refcnt 2 transport_state active,stop,fabric_stop ... INFO: task kworker/0:2:49 blocked for more than 491 seconds. task:kworker/0:2 state:D stack: 0 pid: 49 ppid: 2 flags:0x00000800 Workqueue: events target_tmr_work [target_core_mod] Call Trace: __switch_to+0x2c4/0x470 _schedule+0x314/0x1730 schedule+0x64/0x130 schedule_timeout+0x168/0x430 wait_for_completion+0x140/0x270 target_put_cmd_and_wait+0x64/0xb0 [target_core_mod] core_tmr_lun_reset+0x30/0xa0 [target_core_mod] target_tmr_work+0xc8/0x1b0 [target_core_mod] process_one_work+0x2d4/0x5d0 worker_thread+0x78/0x6c0 To fix this, only add abort to tmr_list if it will be handled by target core. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26833 | In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix memory leak in dm_sw_fini() After destroying dmub_srv, the memory associated with it is not freed, causing a memory leak: unreferenced object 0xffff896302b45800 (size 1024): comm "(udev-worker)", pid 222, jiffies 4294894636 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc 6265fd77): [<ffffffff993495ed>] kmalloc_trace+0x29d/0x340 [<ffffffffc0ea4a94>] dm_dmub_sw_init+0xb4/0x450 [amdgpu] [<ffffffffc0ea4e55>] dm_sw_init+0x15/0x2b0 [amdgpu] [<ffffffffc0ba8557>] amdgpu_device_init+0x1417/0x24e0 [amdgpu] [<ffffffffc0bab285>] amdgpu_driver_load_kms+0x15/0x190 [amdgpu] [<ffffffffc0ba09c7>] amdgpu_pci_probe+0x187/0x4e0 [amdgpu] [<ffffffff9968fd1e>] local_pci_probe+0x3e/0x90 [<ffffffff996918a3>] pci_device_probe+0xc3/0x230 [<ffffffff99805872>] really_probe+0xe2/0x480 [<ffffffff99805c98>] __driver_probe_device+0x78/0x160 [<ffffffff99805daf>] driver_probe_device+0x1f/0x90 [<ffffffff9980601e>] __driver_attach+0xce/0x1c0 [<ffffffff99803170>] bus_for_each_dev+0x70/0xc0 [<ffffffff99804822>] bus_add_driver+0x112/0x210 [<ffffffff99807245>] driver_register+0x55/0x100 [<ffffffff990012d1>] do_one_initcall+0x41/0x300 Fix this by freeing dmub_srv after destroying it. | N/A | More Details |
| CVE-2024-24994 | A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |
| CVE-2024-26834 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_flow_offload: release dst in case direct xmit path is used Direct xmit does not use it since it calls dev_queue_xmit() to send packets, hence it calls dst_release(). kmemleak reports: unreferenced object 0xffff88814f440900 (size 184): comm "softirq", pid 0, jiffies 4294951896 hex dump (first 32 bytes): 00 60 5b 04 81 88 ff ff 00 e6 e8 82 ff ff ff ff .`[..... 21 0b 50 82 ff ff ff ff 00 00 00 00 00 00 00 00 !.P..... backtrace (crc cb2bf5d6): [<000000003ee17107>] kmem_cache_alloc+0x286/0x340 [<0000000021a5de2c>] dst_alloc+0x43/0xb0 [<00000000f0671159>] rt_dst_alloc+0x2e/0x190 [<00000000fe5092c9>] __mkroute_output+0x244/0x980 [<000000005fb96fb0>] ip_route_output_flow+0xc0/0x160 [<0000000045367433>] nf_ip_route+0xf/0x30 [<0000000085da1d8e>] nf_route+0x2d/0x60 [<00000000d1ecd1cb>] nft_flow_route+0x171/0x6a0 [nft_flow_offload] [<00000000d9b2fb60>] nft_flow_offload_eval+0x4e8/0x700 [nft_flow_offload] [<000000009f447dbb>] expr_call_ops_eval+0x53/0x330 [nf_tables] [<00000000072e1be6>] nft_do_chain+0x17c/0x840 [nf_tables] [<00000000d0551029>] nft_do_chain_inet+0xa1/0x210 [nf_tables] [<0000000097c9d5c6>] nf_hook_slow+0x5b/0x160 [<0000000005eccab1>] ip_forward+0x8b6/0x9b0 [<00000000553a269b>] ip_rcv+0x221/0x230 [<00000000412872e5>] __netif_receive_skb_one_core+0xfe/0x110 | N/A | More Details |
| CVE-2024-26835 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: set dormant flag on hook register failure We need to set the dormant flag again if we fail to register the hooks. During memory pressure hook registration can fail and we end up with a table marked as active but no registered hooks. On table/base chain deletion, nf_tables will attempt to unregister the hook again which yields a warn splat from the nftables core. | N/A | More Details |
| CVE-2024-26836 | In the Linux kernel, the following vulnerability has been resolved: platform/x86: think-lmi: Fix password opcode ordering for workstations The Lenovo workstations require the password opcode to be run before the attribute value is changed (if Admin password is enabled). Tested on some Thinkpads to confirm they are OK with this order too. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26837 | In the Linux kernel, the following vulnerability has been resolved: net: bridge: switchdev: Skip MDB replays of deferred events on offload Before this change, generation of the list of MDB events to replay would race against the creation of new group memberships, either from the IGMP/MLD snooping logic or from user configuration. While new memberships are immediately visible to walkers of br->mdb_list, the notification of their existence to switchdev event subscribers is deferred until a later point in time. So if a replay list was generated during a time that overlapped with such a window, it would also contain a replay of the not-yet-delivered event. The driver would thus receive two copies of what the bridge internally considered to be one single event. On destruction of the bridge, only a single membership deletion event was therefore sent. As a consequence of this, drivers which reference count memberships (at least DSA), would be left with orphan groups in their hardware database when the bridge was destroyed. This is only an issue when replaying additions. While deletion events may still be pending on the deferred queue, they will already have been removed from br->mdb_list, so no duplicates can be generated in that scenario. To a user this meant that old group memberships, from a bridge in which a port was previously attached, could be reanimated (in hardware) when the port joined a new bridge, without the new bridge's knowledge. For example, on an mv88e6xxx system, create a snooping bridge and immediately add a port to it: root@infix-06-0b-00:~$ ip link add dev br0 up type bridge mcast_snooping 1 && \ > ip link set dev x3 up master br0 And then destroy the bridge: root@infix-06-0b-00:~$ ip link del dev br0 root@infix-06-0b-00:~$ mvls atu ADDRESS FID STATE Q F 0 1 2 3 4 5 6 7 8 9 a DEV:0 Marvell 88E6393X 33:33:00:00:00:6a 1 static - - 0 . . . . . 33:33:ff:87:e4:3f 1 static - - 0 . . . . . ff:ff:ff:ff:ff:ff 1 static - - 0 1 2 3 4 5 6 7 8 9 a root@infix-06-0b-00:~$ The two IPv6 groups remain in the hardware database because the port (x3) is notified of the host's membership twice: once via the original event and once via a replay. Since only a single delete notification is sent, the count remains at 1 when the bridge is destroyed. Then add the same port (or another port belonging to the same hardware domain) to a new bridge, this time with snooping disabled: root@infix-06-0b-00:~$ ip link add dev br1 up type bridge mcast_snooping 0 && \ > ip link set dev x3 up master br1 All multicast, including the two IPv6 groups from br0, should now be flooded, according to the policy of br1. But instead the old memberships are still active in the hardware database, causing the switch to only forward traffic to those groups towards the CPU (port 0). Eliminate the race in two steps: 1. Grab the write-side lock of the MDB while generating the replay list. This prevents new memberships from showing up while we are generating the replay list. But it leaves the scenario in which a deferred event was already generated, but not delivered, before we grabbed the lock. Therefore: 2. Make sure that no deferred version of a replay event is already enqueued to the switchdev deferred queue, before adding it to the replay list, when replaying additions. | N/A | More Details |
| CVE-2024-26838 | In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Fix KASAN issue with tasklet KASAN testing revealed the following issue assocated with freeing an IRQ. [50006.466686] Call Trace: [50006.466691] <IRQ> [50006.489538] dump_stack+0x5c/0x80 [50006.493475] print_address_description.constprop.6+0x1a/0x150 [50006.499872] ? irdma_sc_process_ceq+0x483/0x790 [irdma] [50006.505742] ? irdma_sc_process_ceq+0x483/0x790 [irdma] [50006.511644] kasan_report.cold.11+0x7f/0x118 [50006.516572] ? irdma_sc_process_ceq+0x483/0x790 [irdma] [50006.522473] irdma_sc_process_ceq+0x483/0x790 [irdma] [50006.528232] irdma_process_ceq+0xb2/0x400 [irdma] [50006.533601] ? irdma_hw_flush_wqes_callback+0x370/0x370 [irdma] [50006.540298] irdma_ceq_dpc+0x44/0x100 [irdma] [50006.545306] tasklet_action_common.isra.14+0x148/0x2c0 [50006.551096] __do_softirq+0x1d0/0xaf8 [50006.555396] irq_exit_rcu+0x219/0x260 [50006.559670] irq_exit+0xa/0x20 [50006.563320] smp_apic_timer_interrupt+0x1bf/0x690 [50006.568645] apic_timer_interrupt+0xf/0x20 [50006.573341] </IRQ> The issue is that a tasklet could be pending on another core racing the delete of the irq. Fix by insuring any scheduled tasklet is killed after deleting the irq. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26839 | In the Linux kernel, the following vulnerability has been resolved: IB/hfi1: Fix a memleak in init_credit_return When dma_alloc_coherent fails to allocate dd->cr_base[i].va, init_credit_return should deallocate dd->cr_base and dd->cr_base[i] that allocated before. Or those resources would be never freed and a memleak is triggered. | N/A | More Details |
| CVE-2024-26844 | In the Linux kernel, the following vulnerability has been resolved: block: Fix WARNING in _copy_from_iter Syzkaller reports a warning in _copy_from_iter because an iov_iter is supposedly used in the wrong direction. The reason is that syzcaller managed to generate a request with a transfer direction of SG_DXFER_TO_FROM_DEV. This instructs the kernel to copy user buffers into the kernel, read into the copied buffers and then copy the data back to user space. Thus the iovec is used in both directions. Detect this situation in the block layer and construct a new iterator with the correct direction for the copy-in. | N/A | More Details |
| CVE-2024-26842 | In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix shift issue in ufshcd_clear_cmd() When task_tag >= 32 (in MCQ mode) and sizeof(unsigned int) == 4, 1U << task_tag will out of bounds for a u32 mask. Fix this up to prevent SHIFT_ISSUE (bitwise shifts that are out of bounds for their data type). [name:debug_monitors&]Unexpected kernel BRK exception at EL1 [name:traps&]Internal error: BRK handler: 00000000f2005514 [#1] PREEMPT SMP [name:mediatek_cpufreq_hw&]cpufreq stop DVFS log done [name:mrdump&]Kernel Offset: 0x1ba5800000 from 0xffffffc008000000 [name:mrdump&]PHYS_OFFSET: 0x80000000 [name:mrdump&]pstate: 22400005 (nzCv daif +PAN -UAO) [name:mrdump&]pc : [0xffffffdbaf52bb2c] ufshcd_clear_cmd+0x280/0x288 [name:mrdump&]lr : [0xffffffdbaf52a774] ufshcd_wait_for_dev_cmd+0x3e4/0x82c [name:mrdump&]sp : ffffffc0081471b0 <snip> Workqueue: ufs_eh_wq_0 ufshcd_err_handler Call trace: dump_backtrace+0xf8/0x144 show_stack+0x18/0x24 dump_stack_lvl+0x78/0x9c dump_stack+0x18/0x44 mrdump_common_die+0x254/0x480 [mrdump] ipanic_die+0x20/0x30 [mrdump] notify_die+0x15c/0x204 die+0x10c/0x5f8 arm64_notify_die+0x74/0x13c do_debug_exception+0x164/0x26c el1_dbg+0x64/0x80 el1h_64_sync_handler+0x3c/0x90 el1h_64_sync+0x68/0x6c ufshcd_clear_cmd+0x280/0x288 ufshcd_wait_for_dev_cmd+0x3e4/0x82c ufshcd_exec_dev_cmd+0x5bc/0x9ac ufshcd_verify_dev_init+0x84/0x1c8 ufshcd_probe_hba+0x724/0x1ce0 ufshcd_host_reset_and_restore+0x260/0x574 ufshcd_reset_and_restore+0x138/0xbd0 ufshcd_err_handler+0x1218/0x2f28 process_one_work+0x5fc/0x1140 worker_thread+0x7d8/0xe20 kthread+0x25c/0x468 ret_from_fork+0x10/0x20 | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26841 | In the Linux kernel, the following vulnerability has been resolved: LoongArch: Update cpu_sibling_map when disabling nonboot CPUs Update cpu_sibling_map when disabling nonboot CPUs by defining & calling clear_cpu_sibling_map(), otherwise we get such errors on SMT systems: jump label: negative count! WARNING: CPU: 6 PID: 45 at kernel/jump_label.c:263 __static_key_slow_dec_cpuslocked+0xec/0x100 CPU: 6 PID: 45 Comm: cpuhp/6 Not tainted 6.8.0-rc5+ #1340 pc 90000000004c302c ra 90000000004c302c tp 90000001005bc000 sp 90000001005bfd20 a0 000000000000001b a1 900000000224c278 a2 90000001005bfb58 a3 900000000224c280 a4 900000000224c278 a5 90000001005bfb50 a6 0000000000000001 a7 0000000000000001 t0 ce87a4763eb5234a t1 ce87a4763eb5234a t2 0000000000000000 t3 0000000000000000 t4 0000000000000006 t5 0000000000000000 t6 0000000000000064 t7 0000000000001964 t8 000000000009ebf6 u0 9000000001f2a068 s9 0000000000000000 s0 900000000246a2d8 s1 ffffffffffffffff s2 ffffffffffffffff s3 90000000021518c0 s4 0000000000000040 s5 9000000002151058 s6 9000000009828e40 s7 00000000000000b4 s8 0000000000000006 ra: 90000000004c302c __static_key_slow_dec_cpuslocked+0xec/0x100 ERA: 90000000004c302c __static_key_slow_dec_cpuslocked+0xec/0x100 CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DACM=CC -WE) PRMD: 00000004 (PPLV0 +PIE -PWE) EUEN: 00000000 (-FPE -SXE -ASXE -BTE) ECFG: 00071c1c (LIE=2-4,10-12 VS=7) ESTAT: 000c0000 [BRK] (IS= ECode=12 EsubCode=0) PRID: 0014d000 (Loongson-64bit, Loongson-3A6000-HV) CPU: 6 PID: 45 Comm: cpuhp/6 Not tainted 6.8.0-rc5+ #1340 Stack : 0000000000000000 900000000203f258 900000000179afc8 90000001005bc000 90000001005bf980 0000000000000000 90000001005bf988 9000000001fe0be0 900000000224c280 900000000224c278 90000001005bf8c0 0000000000000001 0000000000000001 ce87a4763eb5234a 0000000007f38000 90000001003f8cc0 0000000000000000 0000000000000006 0000000000000000 4c206e6f73676e6f 6f4c203a656d616e 000000000009ec99 0000000007f38000 0000000000000000 900000000214b000 9000000001fe0be0 0000000000000004 0000000000000000 0000000000000107 0000000000000009 ffffffffffafdabe 00000000000000b4 0000000000000006 90000000004c302c 9000000000224528 00005555939a0c7c 00000000000000b0 0000000000000004 0000000000000000 0000000000071c1c ... Call Trace: [<9000000000224528>] show_stack+0x48/0x1a0 [<900000000179afc8>] dump_stack_lvl+0x78/0xa0 [<9000000000263ed0>] __warn+0x90/0x1a0 [<90000000017419b8>] report_bug+0x1b8/0x280 [<900000000179c564>] do_bp+0x264/0x420 [<90000000004c302c>] __static_key_slow_dec_cpuslocked+0xec/0x100 [<90000000002b4d7c>] sched_cpu_deactivate+0x2fc/0x300 [<9000000000266498>] cpuhp_invoke_callback+0x178/0x8a0 [<9000000000267f70>] cpuhp_thread_fun+0xf0/0x240 [<90000000002a117c>] smpboot_thread_fn+0x1dc/0x2e0 [<900000000029a720>] kthread+0x140/0x160 [<9000000000222288>] ret_from_kernel_thread+0xc/0xa4 | N/A | More Details |
| CVE-2024-26908 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26906 | In the Linux kernel, the following vulnerability has been resolved: x86/mm: Disallow vsyscall page read for copy_from_kernel_nofault() When trying to use copy_from_kernel_nofault() to read vsyscall page through a bpf program, the following oops was reported: BUG: unable to handle page fault for address: ffffffffff600000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 3231067 P4D 3231067 PUD 3233067 PMD 3235067 PTE 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 20390 Comm: test_progs ..... 6.7.0+ #58 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) ..... RIP: 0010:copy_from_kernel_nofault+0x6f/0x110 ..... Call Trace: <TASK> ? copy_from_kernel_nofault+0x6f/0x110 bpf_probe_read_kernel+0x1d/0x50 bpf_prog_2061065e56845f08_do_probe_read+0x51/0x8d trace_call_bpf+0xc5/0x1c0 perf_call_bpf_enter.isra.0+0x69/0xb0 perf_syscall_enter+0x13e/0x200 syscall_trace_enter+0x188/0x1c0 do_syscall_64+0xb5/0xe0 entry_SYSCALL_64_after_hwframe+0x6e/0x76 </TASK> ..... ---[ end trace 0000000000000000 ]--- The oops is triggered when: 1) A bpf program uses bpf_probe_read_kernel() to read from the vsyscall page and invokes copy_from_kernel_nofault() which in turn calls __get_user_asm(). 2) Because the vsyscall page address is not readable from kernel space, a page fault exception is triggered accordingly. 3) handle_page_fault() considers the vsyscall page address as a user space address instead of a kernel space address. This results in the fix-up setup by bpf not being applied and a page_fault_oops() is invoked due to SMAP. Considering handle_page_fault() has already considered the vsyscall page address as a userspace address, fix the problem by disallowing vsyscall page read for copy_from_kernel_nofault(). | N/A | More Details |
| CVE-2024-30952 | A stored cross-site scripting (XSS) vulnerability in PESCMS-TEAM v2.3.6 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the domain input field under /youdoamin/?g=Team&m=Setting&a=action. | N/A | More Details |
| CVE-2024-26824 | In the Linux kernel, the following vulnerability has been resolved: crypto: algif_hash - Remove bogus SGL free on zero-length error path When a zero-length message is hashed by algif_hash, and an error is triggered, it tries to free an SG list that was never allocated in the first place. Fix this by not freeing the SG list on the zero-length error path. | N/A | More Details |
| CVE-2024-26823 | In the Linux kernel, the following vulnerability has been resolved: irqchip/gic-v3-its: Restore quirk probing for ACPI-based systems While refactoring the way the ITSs are probed, the handling of quirks applicable to ACPI-based platforms was lost. As a result, systems such as HIP07 lose their GICv4 functionnality, and some other may even fail to boot, unless they are configured to boot with DT. Move the enabling of quirks into its_probe_one(), making it common to all firmware implementations. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26851 | In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_h323: Add protection for bmp length out of range UBSAN load reports an exception of BRK#5515 SHIFT_ISSUE:Bitwise shifts that are out of bounds for their data type. vmlinux get_bitmap(b=75) + 712 <net/netfilter/nf_conntrack_h323_asn1.c:0> vmlinux decode_seq(bs=0xFFFFFFD008037000, f=0xFFFFFFD008037018, level=134443100) + 1956 <net/netfilter/nf_conntrack_h323_asn1.c:592> vmlinux decode_choice(base=0xFFFFFFD0080370F0, level=23843636) + 1216 <net/netfilter/nf_conntrack_h323_asn1.c:814> vmlinux decode_seq(f=0xFFFFFFD0080371A8, level=134443500) + 812 <net/netfilter/nf_conntrack_h323_asn1.c:576> vmlinux decode_choice(base=0xFFFFFFD008037280, level=0) + 1216 <net/netfilter/nf_conntrack_h323_asn1.c:814> vmlinux DecodeRasMessage() + 304 <net/netfilter/nf_conntrack_h323_asn1.c:833> vmlinux ras_help() + 684 <net/netfilter/nf_conntrack_h323_main.c:1728> vmlinux nf_confirm() + 188 <net/netfilter/nf_conntrack_proto.c:137> Due to abnormal data in skb->data, the extension bitmap length exceeds 32 when decoding ras message then uses the length to make a shift operation. It will change into negative after several loop. UBSAN load could detect a negative shift as an undefined behaviour and reports exception. So we add the protection to avoid the length exceeding 32. Or else it will return out of range error and stop decoding. | N/A | More Details |
| CVE-2024-26859 | In the Linux kernel, the following vulnerability has been resolved: net/bnx2x: Prevent access to a freed page in page_pool Fix race condition leading to system crash during EEH error handling During EEH error recovery, the bnx2x driver's transmit timeout logic could cause a race condition when handling reset tasks. The bnx2x_tx_timeout() schedules reset tasks via bnx2x_sp_rtnl_task(), which ultimately leads to bnx2x_nic_unload(). In bnx2x_nic_unload() SGEs are freed using bnx2x_free_rx_sge_range(). However, this could overlap with the EEH driver's attempt to reset the device using bnx2x_io_slot_reset(), which also tries to free SGEs. This race condition can result in system crashes due to accessing freed memory locations in bnx2x_free_rx_sge() 799 static inline void bnx2x_free_rx_sge(struct bnx2x *bp, 800 struct bnx2x_fastpath *fp, u16 index) 801 { 802 struct sw_rx_page *sw_buf = &fp->rx_page_ring[index]; 803 struct page *page = sw_buf->page; .... where sw_buf was set to NULL after the call to dma_unmap_page() by the preceding thread. EEH: Beginning: 'slot_reset' PCI 0011:01:00.0#10000: EEH: Invoking bnx2x->slot_reset() bnx2x: [bnx2x_io_slot_reset:14228(eth1)]IO slot reset initializing... bnx2x 0011:01:00.0: enabling device (0140 -> 0142) bnx2x: [bnx2x_io_slot_reset:14244(eth1)]IO slot reset --> driver unload Kernel attempted to read user page (0) - exploit attempt? (uid: 0) BUG: Kernel NULL pointer dereference on read at 0x00000000 Faulting instruction address: 0xc0080000025065fc Oops: Kernel access of bad area, sig: 11 [#1] ..... Call Trace: [c000000003c67a20] [c00800000250658c] bnx2x_io_slot_reset+0x204/0x610 [bnx2x] (unreliable) [c000000003c67af0] [c0000000000518a8] eeh_report_reset+0xb8/0xf0 [c000000003c67b60] [c000000000052130] eeh_pe_report+0x180/0x550 [c000000003c67c70] [c00000000005318c] eeh_handle_normal_event+0x84c/0xa60 [c000000003c67d50] [c000000000053a84] eeh_event_handler+0xf4/0x170 [c000000003c67da0] [c000000000194c58] kthread+0x1c8/0x1d0 [c000000003c67e10] [c00000000000cf64] ret_from_kernel_thread+0x5c/0x64 To solve this issue, we need to verify page pool allocations before freeing. | N/A | More Details |
| CVE-2024-26920 | In the Linux kernel, the following vulnerability has been resolved: tracing/trigger: Fix to return error if failed to alloc snapshot Fix register_snapshot_trigger() to return error code if it failed to allocate a snapshot instead of 0 (success). Unless that, it will register snapshot trigger without an error. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26858 | In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Use a memory barrier to enforce PTP WQ xmit submission tracking occurs after populating the metadata_map Just simply reordering the functions mlx5e_ptp_metadata_map_put and mlx5e_ptpsq_track_metadata in the mlx5e_txwqe_complete context is not good enough since both the compiler and CPU are free to reorder these two functions. If reordering does occur, the issue that was supposedly fixed by 7e3f3ba97e6c ("net/mlx5e: Track xmit submission to PTP WQ after populating metadata map") will be seen. This will lead to NULL pointer dereferences in mlx5e_ptpsq_mark_ts_cqes_undelivered in the NAPI polling context due to the tracking list being populated before the metadata map. | N/A | More Details |
| CVE-2024-26856 | In the Linux kernel, the following vulnerability has been resolved: net: sparx5: Fix use after free inside sparx5_del_mact_entry Based on the static analyzis of the code it looks like when an entry from the MAC table was removed, the entry was still used after being freed. More precise the vid of the mac_entry was used after calling devm_kfree on the mac_entry. The fix consists in first using the vid of the mac_entry to delete the entry from the HW and after that to free it. | N/A | More Details |
| CVE-2024-26855 | In the Linux kernel, the following vulnerability has been resolved: net: ice: Fix potential NULL pointer dereference in ice_bridge_setlink() The function ice_bridge_setlink() may encounter a NULL pointer dereference if nlmsg_find_attr() returns NULL and br_spec is dereferenced subsequently in nla_for_each_nested(). To address this issue, add a check to ensure that br_spec is not NULL before proceeding with the nested attribute iteration. | N/A | More Details |
| CVE-2024-26919 | In the Linux kernel, the following vulnerability has been resolved: usb: ulpi: Fix debugfs directory leak The ULPI per-device debugfs root is named after the ulpi device's parent, but ulpi_unregister_interface tries to remove a debugfs directory named after the ulpi device itself. This results in the directory sticking around and preventing subsequent (deferred) probes from succeeding. Change the directory name to match the ulpi device. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26853 | In the Linux kernel, the following vulnerability has been resolved: igc: avoid returning frame twice in XDP_REDIRECT When a frame can not be transmitted in XDP_REDIRECT (e.g. due to a full queue), it is necessary to free it by calling xdp_return_frame_rx_napi. However, this is the responsibility of the caller of the ndo_xdp_xmit (see for example bq_xmit_all in kernel/bpf/devmap.c) and thus calling it inside igc_xdp_xmit (which is the ndo_xdp_xmit of the igc driver) as well will lead to memory corruption. In fact, bq_xmit_all expects that it can return all frames after the last successfully transmitted one. Therefore, break for the first not transmitted frame, but do not call xdp_return_frame_rx_napi in igc_xdp_xmit. This is equally implemented in other Intel drivers such as the igb. There are two alternatives to this that were rejected: 1. Return num_frames as all the frames would have been transmitted and release them inside igc_xdp_xmit. While it might work technically, it is not what the return value is meant to represent (i.e. the number of SUCCESSFULLY transmitted packets). 2. Rework kernel/bpf/devmap.c and all drivers to support non-consecutively dropped packets. Besides being complex, it likely has a negative performance impact without a significant gain since it is anyway unlikely that the next frame can be transmitted if the previous one was dropped. The memory corruption can be reproduced with the following script which leads to a kernel panic after a few seconds. It basically generates more traffic than a i225 NIC can transmit and pushes it via XDP_REDIRECT from a virtual interface to the physical interface where frames get dropped. #!/bin/bash INTERFACE=enp4s0 INTERFACE_IDX=`cat /sys/class/net/$INTERFACE/ifindex` sudo ip link add dev veth1 type veth peer name veth2 sudo ip link set up $INTERFACE sudo ip link set up veth1 sudo ip link set up veth2 cat << EOF > redirect.bpf.c SEC("prog") int redirect(struct xdp_md *ctx) { return bpf_redirect($INTERFACE_IDX, 0); } char _license[] SEC("license") = "GPL"; EOF clang -O2 -g -Wall -target bpf -c redirect.bpf.c -o redirect.bpf.o sudo ip link set veth2 xdp obj redirect.bpf.o cat << EOF > pass.bpf.c SEC("prog") int pass(struct xdp_md *ctx) { return XDP_PASS; } char _license[] SEC("license") = "GPL"; EOF clang -O2 -g -Wall -target bpf -c pass.bpf.c -o pass.bpf.o sudo ip link set $INTERFACE xdp obj pass.bpf.o cat << EOF > trafgen.cfg { /* Ethernet Header */ 0xe8, 0x6a, 0x64, 0x41, 0xbf, 0x46, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, const16(ETH_P_IP), /* IPv4 Header */ 0b01000101, 0, # IPv4 version, IHL, TOS const16(1028), # IPv4 total length (UDP length + 20 bytes (IP header)) const16(2), # IPv4 ident 0b01000000, 0, # IPv4 flags, fragmentation off 64, # IPv4 TTL 17, # Protocol UDP csumip(14, 33), # IPv4 checksum /* UDP Header */ 10, 0, 1, 1, # IP Src - adapt as needed 10, 0, 1, 2, # IP Dest - adapt as needed const16(6666), # UDP Src Port const16(6666), # UDP Dest Port const16(1008), # UDP length (UDP header 8 bytes + payload length) csumudp(14, 34), # UDP checksum /* Payload */ fill('W', 1000), } EOF sudo trafgen -i trafgen.cfg -b3000MB -o veth1 --cpp | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26892 | In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921e: fix use-after-free in free_irq() From commit a304e1b82808 ("[PATCH] Debug shared irqs"), there is a test to make sure the shared irq handler should be able to handle the unexpected event after deregistration. For this case, let's apply MT76_REMOVED flag to indicate the device was removed and do not run into the resource access anymore. BUG: KASAN: use-after-free in mt7921_irq_handler+0xd8/0x100 [mt7921e] Read of size 8 at addr ffff88824a7d3b78 by task rmmod/11115 CPU: 28 PID: 11115 Comm: rmmod Tainted: G W L 5.17.0 #10 Hardware name: Micro-Star International Co., Ltd. MS-7D73/MPG B650I EDGE WIFI (MS-7D73), BIOS 1.81 01/05/2024 Call Trace: <TASK> dump_stack_lvl+0x6f/0xa0 print_address_description.constprop.0+0x1f/0x190 ? mt7921_irq_handler+0xd8/0x100 [mt7921e] ? mt7921_irq_handler+0xd8/0x100 [mt7921e] kasan_report.cold+0x7f/0x11b ? mt7921_irq_handler+0xd8/0x100 [mt7921e] mt7921_irq_handler+0xd8/0x100 [mt7921e] free_irq+0x627/0xaa0 devm_free_irq+0x94/0xd0 ? devm_request_any_context_irq+0x160/0x160 ? kobject_put+0x18d/0x4a0 mt7921_pci_remove+0x153/0x190 [mt7921e] pci_device_remove+0xa2/0x1d0 __device_release_driver+0x346/0x6e0 driver_detach+0x1ef/0x2c0 bus_remove_driver+0xe7/0x2d0 ? __check_object_size+0x57/0x310 pci_unregister_driver+0x26/0x250 __do_sys_delete_module+0x307/0x510 ? free_module+0x6a0/0x6a0 ? fpregs_assert_state_consistent+0x4b/0xb0 ? rcu_read_lock_sched_held+0x10/0x70 ? syscall_enter_from_user_mode+0x20/0x70 ? trace_hardirqs_on+0x1c/0x130 do_syscall_64+0x5c/0x80 ? trace_hardirqs_on_prepare+0x72/0x160 ? do_syscall_64+0x68/0x80 ? trace_hardirqs_on_prepare+0x72/0x160 entry_SYSCALL_64_after_hwframe+0x44/0xae | N/A | More Details |
| CVE-2024-26917 | In the Linux kernel, the following vulnerability has been resolved: scsi: Revert "scsi: fcoe: Fix potential deadlock on &fip->ctlr_lock" This reverts commit 1a1975551943f681772720f639ff42fbaa746212. This commit causes interrupts to be lost for FCoE devices, since it changed sping locks from "bh" to "irqsave". Instead, a work queue should be used, and will be addressed in a separate commit. | N/A | More Details |
| CVE-2024-26916 | In the Linux kernel, the following vulnerability has been resolved: Revert "drm/amd: flush any delayed gfxoff on suspend entry" commit ab4750332dbe ("drm/amdgpu/sdma5.2: add begin/end_use ring callbacks") caused GFXOFF control to be used more heavily and the codepath that was removed from commit 0dee72639533 ("drm/amd: flush any delayed gfxoff on suspend entry") now can be exercised at suspend again. Users report that by using GNOME to suspend the lockscreen trigger will cause SDMA traffic and the system can deadlock. This reverts commit 0dee726395333fea833eaaf838bc80962df886c8. | N/A | More Details |
| CVE-2024-26914 | In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix incorrect mpc_combine array size [why] MAX_SURFACES is per stream, while MAX_PLANES is per asic. The mpc_combine is an array that records all the planes per asic. Therefore MAX_PLANES should be used as the array size. Using MAX_SURFACES causes array overflow when there are more than 3 planes. [how] Use the MAX_PLANES for the mpc_combine array size. | N/A | More Details |
| CVE-2024-32205 | Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Details |
| CVE-2024-31666 | An issue in flusity-CMS v.2.33 allows a remote attacker to execute arbitrary code via a crafted script to the edit_addon_post.php component. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26822 | In the Linux kernel, the following vulnerability has been resolved: smb: client: set correct id, uid and cruid for multiuser automounts When uid, gid and cruid are not specified, we need to dynamically set them into the filesystem context used for automounting otherwise they'll end up reusing the values from the parent mount. | N/A | More Details |
| CVE-2024-26850 | In the Linux kernel, the following vulnerability has been resolved: mm/debug_vm_pgtable: fix BUG_ON with pud advanced test Architectures like powerpc add debug checks to ensure we find only devmap PUD pte entries. These debug checks are only done with CONFIG_DEBUG_VM. This patch marks the ptes used for PUD advanced test devmap pte entries so that we don't hit on debug checks on architecture like ppc64 as below. WARNING: CPU: 2 PID: 1 at arch/powerpc/mm/book3s64/radix_pgtable.c:1382 radix__pud_hugepage_update+0x38/0x138 .... NIP [c0000000000a7004] radix__pud_hugepage_update+0x38/0x138 LR [c0000000000a77a8] radix__pudp_huge_get_and_clear+0x28/0x60 Call Trace: [c000000004a2f950] [c000000004a2f9a0] 0xc000000004a2f9a0 (unreliable) [c000000004a2f980] [000d34c100000000] 0xd34c100000000 [c000000004a2f9a0] [c00000000206ba98] pud_advanced_tests+0x118/0x334 [c000000004a2fa40] [c00000000206db34] debug_vm_pgtable+0xcbc/0x1c48 [c000000004a2fc10] [c00000000000fd28] do_one_initcall+0x60/0x388 Also kernel BUG at arch/powerpc/mm/book3s64/pgtable.c:202! .... NIP [c000000000096510] pudp_huge_get_and_clear_full+0x98/0x174 LR [c00000000206bb34] pud_advanced_tests+0x1b4/0x334 Call Trace: [c000000004a2f950] [000d34c100000000] 0xd34c100000000 (unreliable) [c000000004a2f9a0] [c00000000206bb34] pud_advanced_tests+0x1b4/0x334 [c000000004a2fa40] [c00000000206db34] debug_vm_pgtable+0xcbc/0x1c48 [c000000004a2fc10] [c00000000000fd28] do_one_initcall+0x60/0x388 | N/A | More Details |
| CVE-2024-26849 | In the Linux kernel, the following vulnerability has been resolved: netlink: add nla be16/32 types to minlen array BUG: KMSAN: uninit-value in nla_validate_range_unsigned lib/nlattr.c:222 [inline] BUG: KMSAN: uninit-value in nla_validate_int_range lib/nlattr.c:336 [inline] BUG: KMSAN: uninit-value in validate_nla lib/nlattr.c:575 [inline] BUG: KMSAN: uninit-value in __nla_validate_parse+0x2e20/0x45c0 lib/nlattr.c:631 nla_validate_range_unsigned lib/nlattr.c:222 [inline] nla_validate_int_range lib/nlattr.c:336 [inline] validate_nla lib/nlattr.c:575 [inline] ... The message in question matches this policy: [NFTA_TARGET_REV] = NLA_POLICY_MAX(NLA_BE32, 255), but because NLA_BE32 size in minlen array is 0, the validation code will read past the malformed (too small) attribute. Note: Other attributes, e.g. BITFIELD32, SINT, UINT.. are also missing: those likely should be added too. | N/A | More Details |
| CVE-2023-52642 | In the Linux kernel, the following vulnerability has been resolved: media: rc: bpf attach/detach requires write permission Note that bpf attach/detach also requires CAP_NET_ADMIN. | N/A | More Details |
| CVE-2023-38302 | A certain software build for the Sharp Rouvo V device (SHARP/VZW_STTM21VAPP/STTM21VAPP:12/SP1A.210812.016/1KN0_0_530:user/release-keys) leaks the Wi-Fi MAC address and the Bluetooth MAC address to system properties that can be accessed by any local app on the device without any permissions or special privileges. Google restricted third-party apps from directly obtaining non-resettable device identifiers in Android 10 and higher, but in this instance they are leaked by a high-privilege process and can be obtained indirectly. This malicious app reads from the "ro.boot.wifi_mac" system property to indirectly obtain the Wi-Fi MAC address and reads the "ro.boot.bt_mac" system property to obtain the Bluetooth MAC address. | N/A | More Details |
| CVE-2024-26848 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-52644 | In the Linux kernel, the following vulnerability has been resolved: wifi: b43: Stop/wake correct queue in DMA Tx path when QoS is disabled When QoS is disabled, the queue priority value will not map to the correct ieee80211 queue since there is only one queue. Stop/wake queue 0 when QoS is disabled to prevent trying to stop/wake a non-existent queue and failing to stop/wake the actual queue instantiated. Log of issue before change (with kernel parameter qos=0): [ +5.112651] ------------[ cut here ]------------ [ +0.000005] WARNING: CPU: 7 PID: 25513 at net/mac80211/util.c:449 __ieee80211_wake_queue+0xd5/0x180 [mac80211] [ +0.000067] Modules linked in: b43(O) snd_seq_dummy snd_hrtimer snd_seq snd_seq_device nft_chain_nat xt_MASQUERADE nf_nat xfrm_user xfrm_algo xt_addrtype overlay ccm af_packet amdgpu snd_hda_codec_cirrus snd_hda_codec_generic ledtrig_audio drm_exec amdxcp gpu_sched xt_conntrack nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ip6t_rpfilter ipt_rpfilter xt_pkttype xt_LOG nf_log_syslog xt_tcpudp nft_compat nf_tables nfnetlink sch_fq_codel btusb uinput iTCO_wdt ctr btrtl intel_pmc_bxt i915 intel_rapl_msr mei_hdcp mei_pxp joydev at24 watchdog btintel atkbd libps2 serio radeon btbcm vivaldi_fmap btmtk intel_rapl_common snd_hda_codec_hdmi bluetooth uvcvideo nls_iso8859_1 applesmc nls_cp437 x86_pkg_temp_thermal snd_hda_intel intel_powerclamp vfat videobuf2_vmalloc coretemp fat snd_intel_dspcfg crc32_pclmul uvc polyval_clmulni snd_intel_sdw_acpi loop videobuf2_memops snd_hda_codec tun drm_suballoc_helper polyval_generic drm_ttm_helper drm_buddy tap ecdh_generic videobuf2_v4l2 gf128mul macvlan ttm ghash_clmulni_intel ecc tg3 [ +0.000044] videodev bridge snd_hda_core rapl crc16 drm_display_helper cec mousedev snd_hwdep evdev intel_cstate bcm5974 hid_appleir videobuf2_common stp mac_hid libphy snd_pcm drm_kms_helper acpi_als mei_me intel_uncore llc mc snd_timer intel_gtt industrialio_triggered_buffer apple_mfi_fastcharge i2c_i801 mei snd lpc_ich agpgart ptp i2c_smbus thunderbolt apple_gmux i2c_algo_bit kfifo_buf video industrialio soundcore pps_core wmi tiny_power_button sbs sbshc button ac cordic bcma mac80211 cfg80211 ssb rfkill libarc4 kvm_intel kvm drm irqbypass fuse backlight firmware_class efi_pstore configfs efivarfs dmi_sysfs ip_tables x_tables autofs4 dm_crypt cbc encrypted_keys trusted asn1_encoder tee tpm rng_core input_leds hid_apple led_class hid_generic usbhid hid sd_mod t10_pi crc64_rocksoft crc64 crc_t10dif crct10dif_generic ahci libahci libata uhci_hcd ehci_pci ehci_hcd crct10dif_pclmul crct10dif_common sha512_ssse3 sha512_generic sha256_ssse3 sha1_ssse3 aesni_intel usbcore scsi_mod libaes crypto_simd cryptd scsi_common [ +0.000055] usb_common rtc_cmos btrfs blake2b_generic libcrc32c crc32c_generic crc32c_intel xor raid6_pq dm_snapshot dm_bufio dm_mod dax [last unloaded: b43(O)] [ +0.000009] CPU: 7 PID: 25513 Comm: irq/17-b43 Tainted: G W O 6.6.7 #1-NixOS [ +0.000003] Hardware name: Apple Inc. MacBookPro8,3/Mac-942459F5819B171B, BIOS 87.0.0.0.0 06/13/2019 [ +0.000001] RIP: 0010:__ieee80211_wake_queue+0xd5/0x180 [mac80211] [ +0.000046] Code: 00 45 85 e4 0f 85 9b 00 00 00 48 8d bd 40 09 00 00 f0 48 0f ba ad 48 09 00 00 00 72 0f 5b 5d 41 5c 41 5d 41 5e e9 cb 6d 3c d0 <0f> 0b 5b 5d 41 5c 41 5d 41 5e c3 cc cc cc cc 48 8d b4 16 94 00 00 [ +0.000002] RSP: 0018:ffffc90003c77d60 EFLAGS: 00010097 [ +0.000001] RAX: 0000000000000001 RBX: 0000000000000002 RCX: 0000000000000000 [ +0.000001] RDX: 0000000000000000 RSI: 0000000000000002 RDI: ffff88820b924900 [ +0.000002] RBP: ffff88820b924900 R08: ffffc90003c77d90 R09: 000000000003bfd0 [ +0.000001] R10: ffff88820b924900 R11: ffffc90003c77c68 R12: 0000000000000000 [ +0.000001] R13: 0000000000000000 R14: ffffc90003c77d90 R15: ffffffffc0fa6f40 [ +0.000001] FS: 0000000000000000(0000) GS:ffff88846fb80000(0000) knlGS:0000000000000000 [ +0.000001] CS: 0010 DS: 0 ---truncated--- | N/A | More Details |
| CVE-2023-52643 | In the Linux kernel, the following vulnerability has been resolved: iio: core: fix memleak in iio_device_register_sysfs When iio_device_register_sysfs_group() fails, we should free iio_dev_opaque->chan_attr_group.attrs to prevent potential memleak. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2024-26893 | In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix double free in SMC transport cleanup path When the generic SCMI code tears down a channel, it calls the chan_free callback function, defined by each transport. Since multiple protocols might share the same transport_info member, chan_free() might want to clean up the same member multiple times within the given SCMI transport implementation. In this case, it is SMC transport. This will lead to a NULL pointer dereference at the second time: l scmi_protocol scmi_dev.1: Enabled polling mode TX channel - prot_id:16 l arm-scmi firmware:scmi: SCMI Notifications - Core Enabled. l arm-scmi firmware:scmi: unable to communicate with SCMI l Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 l Mem abort info: l ESR = 0x0000000096000004 l EC = 0x25: DABT (current EL), IL = 32 bits l SET = 0, FnV = 0 l EA = 0, S1PTW = 0 l FSC = 0x04: level 0 translation fault l Data abort info: l ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 l CM = 0, WnR = 0, TnD = 0, TagAccess = 0 l GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 l user pgtable: 4k pages, 48-bit VAs, pgdp=0000000881ef8000 l [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 l Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP l Modules linked in: l CPU: 4 PID: 1 Comm: swapper/0 Not tainted 6.7.0-rc2-00124-g455ef3d016c9-dirty #793 l Hardware name: FVP Base RevC (DT) l pstate: 61400009 (nZCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) l pc : smc_chan_free+0x3c/0x6c l lr : smc_chan_free+0x3c/0x6c l Call trace: l smc_chan_free+0x3c/0x6c l idr_for_each+0x68/0xf8 l scmi_cleanup_channels.isra.0+0x2c/0x58 l scmi_probe+0x434/0x734 l platform_probe+0x68/0xd8 l really_probe+0x110/0x27c l __driver_probe_device+0x78/0x12c l driver_probe_device+0x3c/0x118 l __driver_attach+0x74/0x128 l bus_for_each_dev+0x78/0xe0 l driver_attach+0x24/0x30 l bus_add_driver+0xe4/0x1e8 l driver_register+0x60/0x128 l __platform_driver_register+0x28/0x34 l scmi_driver_init+0x84/0xc0 l do_one_initcall+0x78/0x33c l kernel_init_freeable+0x2b8/0x51c l kernel_init+0x24/0x130 l ret_from_fork+0x10/0x20 l Code: f0004701 910a0021 aa1403e5 97b91c70 (b9400280) l ---[ end trace 0000000000000000 ]--- Simply check for the struct pointer being NULL before trying to access its members, to avoid this situation. This was found when a transport doesn't really work (for instance no SMC service), the probe routines then tries to clean up, and triggers a crash. | N/A | More Details |
| CVE-2024-26818 | In the Linux kernel, the following vulnerability has been resolved: tools/rtla: Fix clang warning about mount_point var size clang is reporting this warning: $ make HOSTCC=clang CC=clang LLVM_IAS=1 [...] clang -O -g -DVERSION=\"6.8.0-rc3\" -flto=auto -fexceptions -fstack-protector-strong -fasynchronous-unwind-tables -fstack-clash-protection -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS $(pkg-config --cflags libtracefs) -c -o src/utils.o src/utils.c src/utils.c:548:66: warning: 'fscanf' may overflow; destination buffer in argument 3 has size 1024, but the corresponding specifier may require size 1025 [-Wfortify-source] 548 l while (fscanf(fp, "%*s %" STR(MAX_PATH) "s %99s %*s %*d %*d\n", mount_point, type) == 2) { l ^ Increase mount_point variable size to MAX_PATH+1 to avoid the overflow. | N/A | More Details |
| CVE-2024-26819 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |
| CVE-2024-26820 | In the Linux kernel, the following vulnerability has been resolved: hv_netvsc: Register VF in netvsc_probe if NET_DEVICE_REGISTER missed If hv_netvsc driver is unloaded and reloaded, the NET_DEVICE_REGISTER handler cannot perform VF register successfully as the register call is received before netvsc_probe is finished. This is because we register register_netdevice_notifier() very early( even before vmbus_driver_register()). To fix this, we try to register each such matching VF( if it is visible as a netdevice) at the end of netvsc_probe. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2024-26821 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | More Details |
| CVE-2024-24993 | A Race Condition (TOCTOU) vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM. | N/A | More Details |