SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 29 March 2023

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-2023-28444 | angular-server-side-configuration helps configure an angular application at runtime on the server or in a docker container via environment variables. angular-server-side-configuration detects used environment variables in TypeScript (.ts) files during build time of an Angular CLI project. The detected environment variables are written to a ngssc.json file in the output directory. During deployment of an Angular based app, the environment variables based on the variables from ngssc.json are inserted into the apps index.html (or defined index file). With version 15.0.0 the environment variable detection was widened to the entire project, relative to the angular.json file from the Angular CLI. In a monorepo setup, this could lead to environment variables intended for a backend/service to be detected and written to the ngssc.json, which would then be populated and exposed via index.html. This has NO IMPACT, in a plain Angular project that has no backend component. This vulnerability has been mitigated in version 15.1.0, by adding an option `searchPattern` which restricts the detection file range by default. As a workaround, manually edit or create ngssc.json or run script after ngssc.json generation. | 9.9 | More Details |
| CVE-2023-28445 | Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers. | 9.9 | More Details |
| CVE-2022-3682 | A vulnerability exists in the SDM600 file permission validation. An attacker could exploit the vulnerability by gaining access to the system and uploading a specially crafted message to the system node, which could result in Arbitrary code Executing. This issue affects: All SDM600 versions prior to version 1.2 FP3 HF4 (Build Nr. 1.2.23000.291) List of CPEs: * cpe:2.3:a:hitachienergy:sdm600:1.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.1:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.9002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.10002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.11002.149:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.12002.222:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.13002.72:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.44:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.92:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.108:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.182:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.342:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.447:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.481:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.506:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.566:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.20000.3174:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.291:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.931:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.105:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.23000.291:*:*:*:*:*:*:* | 9.9 | More Details |
| CVE-2023-25261 | Certain Stimulsoft GmbH products are affected by: Remote Code Execution. This affects Stimulsoft Designer (Desktop) 2023.1.4 and Stimulsoft Designer (Web) 2023.1.3 and Stimulsoft Viewer (Web) 2023.1.3. Access to the local file system is not prohibited in any way. Therefore, an attacker may include source code which reads or writes local directories and files. It is also possible for the attacker to prepare a report which has a variable that holds the gathered data and render it in the report. | 9.8 | More Details |
| CVE-2023-27847 | SQL injection vulnerability found in PrestaShop xipblog v.2.0.1 and before allow a remote attacker to gain privileges via the xipcategoryclass and xippostsclass components. | 9.8 | More Details |
| CVE-2023-1140 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability that could allow an attacker to achieve unauthenticated remote code execution in the context of an administrator. | 9.8 | More Details |
| CVE-2023-1136 | In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an unauthenticated attacker could generate a valid token, which would lead to authentication bypass. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1133 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability in which the Device-status service listens on port 10100/ UDP by default. The service accepts the unverified UDP packets and deserializes the content, which could allow an unauthenticated attacker to remotely execute arbitrary code. | 9.8 | More Details |
| CVE-2023-26959 | Phpgurukul Park Ticketing Management System 1.0 is vulnerable to SQL Injection via the User Name parameter. | 9.8 | More Details |
| CVE-2023-25909 | HGiga OAKlouds file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary command or disrupt service. | 9.8 | More Details |
| CVE-2023-27855 | In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. | 9.8 | More Details |
| CVE-2022-48353 | Some smartphones have configuration issues. Successful exploitation of this vulnerability may cause kernel privilege escalation, which results in system service exceptions. | 9.8 | More Details |
| CVE-2023-28883 | In Cerebrate 1.13, a blind SQL injection exists in the searchAll API endpoint. | 9.8 | More Details |
| CVE-2018-25083 | The pullit package before 1.4.0 for Node.js allows OS Command Injection because eval is used on an attacker-supplied Git branch name. | 9.8 | More Details |
| CVE-2023-26802 | An issue in the component /network_config/nsg_masq.cgi of DCN (Digital China Networks) DCBI-Netlog-LAB v1.0 allows attackers to bypass authentication and execute arbitrary commands via a crafted request. | 9.8 | More Details |
| CVE-2023-26801 | LB-LINK BL-AC1900_2.0 v1.0.1, LB-LINK BL-WR9000 v2.4.9, LB-LINK BL-X26 v1.2.5, and LB-LINK BL-LTE300 v1.0.8 were discovered to contain a command injection vulnerability via the mac, time1, and time2 parameters at /goform/set_LimitClient_cfg. | 9.8 | More Details |
| CVE-2023-26800 | Ruijie Networks RG-EW1200 Wireless Routers EW_3.0(1)B11P204 was discovered to contain a command injetion vulnerability via the params.path parameter in the upgradeConfirm function. | 9.8 | More Details |
| CVE-2023-28437 | Dataease is an open source data visualization and analysis tool. The blacklist for SQL injection protection is missing entries. This vulnerability has been fixed in version 1.18.5. There are no known workarounds. | 9.8 | More Details |
| CVE-2023-25668 | TensorFlow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.11.1. | 9.8 | More Details |
| CVE-2023-23149 | DEK-1705 <=Firmware:34.23.1 device was discovered to have a command execution vulnerability. | 9.8 | More Details |
| CVE-2023-24838 | HGiga PowerStation has a vulnerability of Information Leakage. An unauthenticated remote attacker can exploit this vulnerability to obtain the administrator's credential. This credential can then be used to login PowerStation or Secure Shell to achieve remote code execution. | 9.8 | More Details |
| CVE-2023-1665 | Improper Restriction of Excessive Authentication Attempts in GitHub repository linagora/twake prior to 0.0.0. | 9.8 | More Details |
| CVE-2023-28326 | Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 2.0.0 before 7.0.0 Description: Attacker can elevate their privileges in any room | 9.8 | More Details |
| CVE-2023-27821 | Databasir v1.0.7 was discovered to contain a remote code execution (RCE) vulnerability via the mockDataScript parameter. | 9.8 | More Details |
| CVE-2023-27231 | TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the downBw parameter at /setting/setWanIeCfg. | 9.8 | More Details |
| CVE-2023-27229 | TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the upBw parameter at /setting/setWanIeCfg. | 9.8 | More Details |
| CVE-2022-45460 | Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow an unauthenticated and remote user to exploit a stack-based buffer overflow and crash the web server, resulting in a system reboot. An unauthenticated and remote attacker can execute arbitrary code by sending a crafted HTTP request that triggers the overflow condition via a long URI passed to a sprintf call. NOTE: this is different than CVE-2018-10088, but this may overlap CVE-2017-16725. | 9.8 | More Details |
| CVE-2023-28654 | Osprey Pump Controller version 1.01 has a hidden administrative account that has the hardcoded password that allows full access to the web management interface configuration. The user is not visible in Usernames and Passwords menu list of the application and the password cannot be changed through any normal operation of the device. | 9.8 | More Details |
| CVE-2023-28398 | Osprey Pump Controller version 1.01 could allow an unauthenticated user to create an account and bypass authentication, thereby gaining unauthorized access to the system. A threat actor could exploit this vulnerability to create a user account without providing valid credentials. A threat actor who successfully exploits this vulnerability could gain access to the pump controller and cause disruption in operation, modify data, or shut down the controller. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27886 | Osprey Pump Controller version 1.01 is vulnerable to an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through a HTTP POST parameter called by index.php script. | 9.8 | More Details |
| CVE-2023-27394 | Osprey Pump Controller version 1.01 is vulnerable an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through a HTTP GET parameter called by DataLogView.php, EventsView.php and AlarmsView.php scripts. | 9.8 | More Details |
| CVE-2022-46387 | ConEmu through 220807 and Cmder before 1.3.21 report the title of the terminal, including control characters, which allows an attacker to change the title and then execute it as commands. | 9.8 | More Details |
| CVE-2022-24673 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Canon imageCLASS MF644Cdw 10.02 printers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the SLP protocol. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15845. | 9.8 | More Details |
| CVE-2022-23125 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the copyapplfile function. When parsing the len element, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15869. | 9.8 | More Details |
| CVE-2022-23124 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the get_finderinfo method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-15870. | 9.8 | More Details |
| CVE-2022-23123 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getdirparams method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-15830. | 9.8 | More Details |
| CVE-2022-23122 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the setfilparams function. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15837. | 9.8 | More Details |
| CVE-2022-23121 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parse_entries function. The issue results from the lack of proper error handling when parsing AppleDouble entries. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15819. | 9.8 | More Details |
| CVE-2022-0194 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Netatalk. Authentication is not required to exploit this vulnerability. The specific flaw exists within the ad_addcomment function. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15876. | 9.8 | More Details |
| CVE-2023-26864 | SQL injection vulnerability found in PrestaShop smplredirectionsmanager v.1.1.19 and before allow a remote attacker to gain privileges via the SmplTools::getMatchingRedirectionsFromPartscomponent. | 9.8 | More Details |
| CVE-2022-45597 | ComponentSpace.Saml2 4.4.0 Missing SSL Certificate Validation. NOTE: the vendor does not consider this a vulnerability because the report is only about use of certificates at the application layer (not the transport layer) and "Certificates are exchanged in a controlled fashion between entities within a trust relationship. This is why self-signed certificates may be used and why validating certificates isn't as important as doing so for the transport layer certificates." | 9.8 | More Details |
| CVE-2023-21058 | In lcsm_SendRrAcquiAssist of lcsm_bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-246169606References: N/A | 9.8 | More Details |
| CVE-2023-24655 | Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter under the Profile Update function. | 9.8 | More Details |
| CVE-2022-28497 | TOTOLink outdoor CPE CP900 V6.3c.566_B20171026 is discovered to contain a command injection vulnerability in the mtd_write_bootloader function via the filename parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request. | 9.8 | More Details |
| CVE-2023-27135 | TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the enabled parameter at /setting/setWanIeCfg. | 9.8 | More Details |
| CVE-2023-27078 | A command injection issue was found in TP-Link MR3020 v.1_150921 that allows a remote attacker to execute arbitrary commands via a crafted request to the tftp endpoint. | 9.8 | More Details |
| CVE-2022-28493 | A vulnerability in TOTOLINK CP900 V6.3c.566 allows attackers to start the Telnet service, | 9.8 | More Details |
| CVE-2022-28491 | TOTOLink outdoor CPE CP900 V6.3c.566_B20171026 contains a command injection vulnerability in the NTPSyncWithHost function via the host_name parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request. | 9.8 | More Details |
| CVE-2022-28492 | TOTOLINK Technology CPE with firmware V6.3c.566 ,allows remote attackers to bypass Login. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1050 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in As Koc Energy Web Report System allows SQL Injection.This issue affects Web Report System: before 23.03.10. | 9.8 | More Details |
| CVE-2022-22512 | Hard-coded credentials in Web-UI of multiple VARTA Storage products in multiple versions allows an unauthorized attacker to gain administrative access to the Web-UI via network. | 9.8 | More Details |
| CVE-2022-28494 | TOTOLink outdoor CPE CP900 V6.3c.566_B20171026 is discovered to contain a command injection vulnerability in the setUpgradeFW function via the filename parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request. | 9.8 | More Details |
| CVE-2022-28496 | TOTOLink outdoor CPE CP900 V6.3c.566_B20171026 discovered to contain a command injection vulnerability in the setPasswordCfg function via the adminuser and adminpassparameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request. | 9.8 | More Details |
| CVE-2023-27100 | Improper restriction of excessive authentication attempts in the SSHGuard component of Netgate pfSense Plus software v22.05.1 and pfSense CE software v2.6.0 allows attackers to bypass brute force protection mechanisms via crafted web requests. | 9.8 | More Details |
| CVE-2023-27060 | LightCMS v1.3.7 was discovered to contain a remote code execution (RCE) vulnerability via the image:make function. | 9.8 | More Details |
| CVE-2023-28667 | The Lead Generated WordPress Plugin, version <= 1.23, was affected by an unauthenticated insecure deserialization issue. The tve_labels parameter of the tve_api_form_submit action is passed to the PHP unserialize() function without being sanitized or verified, and as a result could lead to PHP object injection, which when combined with certain class implementations / gadget chains could be leveraged to perform a variety of malicious actions granted a POP chain is also present. | 9.8 | More Details |
| CVE-2023-28662 | The Gift Cards (Gift Vouchers and Packages) WordPress Plugin, version <= 4.3.1, is affected by an unauthenticated SQL injection vulnerability in the template parameter in the wpgv_doajax_voucher_pdf_save_func action. | 9.8 | More Details |
| CVE-2023-27224 | An issue found in NginxProxyManager v.2.9.19 allows an attacker to execute arbitrary code via a lua script to the configuration file. | 9.8 | More Details |
| CVE-2023-27638 | An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with a compromised tshirtecommerce_design_cart_id GET parameter in order to exploit an insecure parameter in the functions hookActionCartSave and updateCustomizationTable, which could lead to a SQL injection. This is exploited in the wild in March 2023. | 9.8 | More Details |
| CVE-2023-27637 | An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with a compromised product_id GET parameter in order to exploit an insecure parameter in the front controller file designer.php, which could lead to a SQL injection. This is exploited in the wild in March 2023. | 9.8 | More Details |
| CVE-2023-25589 | A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise. | 9.8 | More Details |
| CVE-2023-28610 | The update process in OMICRON StationGuard and OMICRON StationScout before 2.21 can be exploited by providing a modified firmware update image. This allows a remote attacker to gain root access to the system. | 9.8 | More Details |
| CVE-2023-27232 | TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the wanStrategy parameter at /setting/setWanIeCfg. | 9.8 | More Details |
| CVE-2023-27034 | PrestaShop jmsblog 2.5.5 was discovered to contain a SQL injection vulnerability. | 9.8 | More Details |
| CVE-2022-42498 | In Pixel cellular firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240662453References: N/A | 9.8 | More Details |
| CVE-2023-21057 | In ProfSixDecomTcpSACKoption of RohcPacketCommon, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244450646References: N/A | 9.8 | More Details |
| CVE-2023-20954 | In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 | 9.8 | More Details |
| CVE-2023-20951 | In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631 | 9.8 | More Details |
| CVE-2023-25654 | baserCMS is a Content Management system. Prior to version 4.7.5, there is a Remote Code Execution (RCE) Vulnerability in the management system of baserCMS. Version 4.7.5 contains a patch. | 9.8 | More Details |
| CVE-2023-25655 | baserCMS is a Content Management system. Prior to version 4.7.5, any file may be uploaded on the management system of baserCMS. Version 4.7.5 contains a patch. | 9.8 | More Details |
| CVE-2023-26359 | Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28333 | The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). | 9.8 | More Details |
| CVE-2023-28611 | Incorrect authorization in OMICRON StationGuard 1.10 through 2.20 and StationScout 1.30 through 2.20 allows an attacker to bypass intended access restrictions. | 9.8 | More Details |
| CVE-2022-42499 | In sms_SendMmCpErrMsg of sms_MmConManagement.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242001391References: N/A | 9.8 | More Details |
| CVE-2022-28495 | TOTOLink outdoor CPE CP900 V6.3c.566_B20171026 is discovered to contain a command injection vulnerability in the setWebWlanIdx function via the webWlanIdx parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request. | 9.8 | More Details |
| CVE-2022-42948 | Cobalt Strike 4.7.1 fails to properly escape HTML tags when they are displayed on Swing components. By injecting crafted HTML code, it is possible to remotely execute code in the Cobalt Strike UI. | 9.8 | More Details |
| CVE-2022-20532 | In parseTrackFragmentRun() of MPEG4Extractor.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-232242894 | 9.8 | More Details |
| CVE-2022-4126 | Use of Default Password vulnerability in ABB RCCMD on Windows, Linux, MacOS allows Try Common or Default Usernames and Passwords.This issue affects RCCMD: before 4.40 230207. | 9.6 | More Details |
| CVE-2023-1177 | Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.2.1. | 9.3 | More Details |
| CVE-2023-28725 | General Bytes Crypto Application Server (CAS) 20230120, as distributed with General Bytes BATM devices, allows remote attackers to execute arbitrary Java code by uploading a Java application to the /batm/app/admin/standalone/deployments directory, aka BATM-4780, as exploited in the wild in March 2023. This is fixed in 20221118.48 and 20230120.44. | 9.1 | More Details |
| CVE-2022-48348 | The MediaProvider module has a vulnerability of unauthorized data read. Successful exploitation of this vulnerability may affect confidentiality and integrity. | 9.1 | More Details |
| CVE-2022-46415 | DJI Spark 01.00.0900 allows remote attackers to prevent legitimate terminal connections by exhausting the DHCP IP address pool. To accomplish this, the attacker would first need to connect to the device's internal Wi-Fi network (e.g., by guessing the password). Then, the attacker would need to send many DHCP request packets. | 9.1 | More Details |
| CVE-2022-46416 | Parrot Bebop 4.7.1. allows remote attackers to prevent legitimate terminal connections by exhausting the DHCP IP address pool. To accomplish this, the attacker would first need to connect to the device's internal Wi-Fi network (e.g., by guessing the password). Then, the attacker would need to send many DHCP request packets. | 9.1 | More Details |
| CVE-2022-36413 | Zoho ManageEngine ADSelfService Plus through 6203 is vulnerable to a brute-force attack that leads to a password reset on IDM applications. | 9.1 | More Details |
| CVE-2022-48349 | The control component has a spoofing vulnerability. Successful exploitation of this vulnerability may affect confidentiality and availability. | 9.1 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1144 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contains an improper access control vulnerability in which an attacker can use the Device-Gateway service and bypass authorization, which could result in privilege escalation. | 8.8 | M D |
| CVE-2022-24674 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Canon imageCLASS MF644Cdw 10.02 printers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the privet API. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15834. | 8.8 | M D |
| CVE-2022-24353 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AC1750 1.1.4 Build 20211022 rel.59103(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko module. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the root user. Was ZDI-CAN-15769. | 8.8 | M D |
| CVE-2022-24352 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AC1750 prior to 211210 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko kernel module. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15773. | 8.8 | M D |
| CVE-2023-27246 | An arbitrary file upload vulnerability in the Virtual Disk of MK-Auth 23.01K4.9 allows attackers to execute arbitrary code via uploading a crafted .htaccess file. | 8.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-0955 | The WP Statistics WordPress plugin before 14.0 does not escape a parameter, which could allow authenticated users to perform SQL Injection attacks. By default, the affected feature is available to users with the manage_options capability (admin+), however the plugin has a settings to allow low privilege users to access it as well. | 8.8 | M D |
| CVE-2020-36666 | The directory-pro WordPress plugin before 1.9.5, final-user-wp-frontend-user-profiles WordPress plugin before 1.2.2, producer-retailer WordPress plugin through TODO, photographer-directory WordPress plugin before 1.0.9, real-estate-pro WordPress plugin before 1.7.1, institutions-directory WordPress plugin before 1.3.1, lawyer-directory WordPress plugin before 1.2.9, doctor-listing WordPress plugin before 1.3.6, Hotel Listing WordPress plugin before 1.3.7, fitness-trainer WordPress plugin before 1.4.1, wp-membership WordPress plugin before 1.5.7, sold by the same developer (e-plugins), do not implementing any security measures in some AJAX calls. For example in the file plugin.php, the function iv_directories_update_profile_setting() uses update_user_meta with any data provided by the ajax call, which can be used to give the logged in user admin capabilities. Since the plugins allow user registration via a custom form (even if the blog does not allow users to register) it makes any site using it vulnerable. | 8.8 | M D |
| CVE-2023-27296 | Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache InLong. It could be triggered by authenticated users of InLong, you could refer to [1] to know more about this vulnerability. This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick [2] to solve it. [1] https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html [2] https://github.com/apache/inlong/pull/7422 https://github.com/apache/inlong/pull/7422 | 8.8 | M D |
| CVE-2020-19786 | File upload vulnerability in CSKaza CSZ CMS v.1.2.2 fixed in v1.2.4 allows attacker to execute aritrary commands and code via crafted PHP file. | 8.8 | M D |
| CVE-2023-1143 | In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could use Lua scripts, which could allow an attacker to remotely execute arbitrary code. | 8.8 | M D |
| CVE-2023-1141 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a command injection vulnerability that could allow an attacker to inject arbitrary commands, which could result in remote code execution. | 8.8 | M D |
| CVE-2023-1139 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a deserialization vulnerability targeting the Device-gateway service, which could allow deserialization of requests prior to authentication, resulting in remote code execution. | 8.8 | M D |
| CVE-2023-1578 | SQL Injection in GitHub repository pimcore/pimcore prior to 10.5.19. | 8.8 | M D |
| CVE-2023-24837 | HGiga PowerStation remote management function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operation or disrupt service. | 8.8 | M D |
| CVE-2023-1647 | Improper Access Control in GitHub repository calcom/cal.com prior to 2.7. | 8.8 | M D |
| CVE-2023-27796 | RG-EW1200G PRO Wireless Routers EW_3.0(1)B11P204, RG-EW1800GX PRO Wireless Routers EW_3.0(1)B11P204, and RG-EW3200GX PRO Wireless Routers EW_3.0(1)B11P204 were discovered to contain multiple command injection vulnerabilities via the data.ip, data.protocal, data.iface and data.package parameters in the runPackDiagnose function of diagnose.lua. | 8.8 | M D |
| CVE-2023-27042 | Tenda AX3 V16.03.12.11 is vulnerable to Buffer Overflow via /goform/SetFirewallCfg. | 8.8 | M D |
| CVE-2023-28446 | Deno is a simple, modern and secure runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Arbitrary program names without any ANSI filtering allows any malicious program to clear the first 2 lines of a `op_spawn_child` or `op_kill` prompt and replace it with any desired text. This works with any command on the respective platform, giving the program the full ability to choose what program they wanted to run. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). This issue has been patched in version 1.31.2. | 8.8 | M D |
| CVE-2023-25350 | Faveo Helpdesk 1.0-1.11.1 is vulnerable to SQL Injection. When the user logs in through the login box, he has no judgment on the validity of the user's input data. The parameters passed from the front end to the back end are controllable, which will lead to SQL injection. | 8.8 | M D |
| CVE-2023-28433 | Minio is a Multi-Cloud Object Storage framework. All users on Windows prior to version RELEASE.2023-03-20T20-16-18Z are impacted. MinIO fails to filter the `\` character, which allows for arbitrary object placement across buckets. As a result, a user with low privileges, such as an access key, service account, or STS credential, which only has permission to `PutObject` in a specific bucket, can create an admin user. This issue is patched in RELEASE.2023-03-20T20-16-18Z. There are no known workarounds. | 8.8 | M D |
| CVE-2023-28434 | Minio is a Multi-Cloud Object Storage framework. Prior to RELEASE.2023-03-20T20-16-18Z, an attacker can use crafted requests to bypass metadata bucket name checking and put an object into any bucket while processing `PostPolicyBucket`. To carry out this attack, the attacker requires credentials with `arn:aws:s3:::*` permission, as well as enabled Console API access. This issue has been patched in RELEASE.2023-03-20T20-16-18Z. As a workaround, enable browser API access and turn off `MINIO_BROWSER=off`. | 8.8 | M D |
| CVE-2023-28659 | The Waiting: One-click Countdowns WordPress Plugin, version <= 0.6.2, is affected by an authenticated SQL injection vulnerability in the pbc_down[meta][id] parameter of the pbc_save_downs action. | 8.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-28660 | The Events Made Easy WordPress Plugin, version <= 2.3.14 is affected by an authenticated SQL injection vulnerability in the 'search_name' parameter in the eme_recurrences_list action. | 8.8 | M D |
| CVE-2023-28661 | The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. | 8.8 | M D |
| CVE-2023-28663 | The Formidable PRO2PDF WordPress Plugin, version < 3.11, is affected by an authenticated SQL injection vulnerability in the ‘fieldmap’ parameter in the fpropdf_export_file action. | 8.8 | M D |
| CVE-2018-25048 | The CODESYS runtime system in multiple versions allows an remote low privileged attacker to use a path traversal vulnerability to access and modify all system files as well as DoS the device. | 8.8 | M D |
| CVE-2022-4224 | In multiple products of CODESYS v3 in multiple versions a remote low privileged user could utilize this vulnerability to read and modify system files and OS resources or DoS the device. | 8.8 | M D |
| CVE-2023-20960 | In launchDeepLinkIntentToRight of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-250589026 | 8.8 | M D |
| CVE-2023-28335 | The link to reset all templates of a database activity did not include the necessary token to prevent a CSRF risk. | 8.8 | M D |
| CVE-2023-28329 | Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). | 8.8 | M D |
| CVE-2023-24788 | NotrinosERP v0.7 was discovered to contain a SQL injection vulnerability via the OrderNumber parameter at /NotrinosERP/sales/customer_delivery.php. | 8.8 | M D |
| CVE-2022-24672 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Canon imageCLASS MF644Cdw 10.02 printers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the CADM service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15802. | 8.8 | M D |
| CVE-2023-27094 | An issue found in OpenGoofy Hippo4j v.1.4.3 allows attackers to escalate privileges via the ThreadPoolController of the tenant Management module. | 8.8 | M D |
| CVE-2023-25069 | TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must first obtain a low-privileged authenticated user's profile on the target system in order to exploit this vulnerability. | 8.8 | M D |
| CVE-2023-20072 | A vulnerability in the fragmentation handling code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. | 8.6 | M D |
| CVE-2023-26496 | An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. | 8.6 | M D |
| CVE-2023-26360 | Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. | 8.6 | M D |
| CVE-2023-20080 | A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. | 8.6 | M D |
| CVE-2023-26498 | An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. | 8.6 | M D |
| CVE-2023-26358 | Creative Cloud version 5.9.1 (and earlier) is affected by an Untrusted Search Path vulnerability that might allow attackers to execute their own programs, access unauthorized data files, or modify configuration in unexpected ways. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. The problem extends to any type of critical resource that the application trusts. | 8.6 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20027 | A vulnerability in the implementation of the IPv4 Virtual Fragmentation Reassembly (VFR) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper reassembly of large packets that occurs when VFR is enabled on either a tunnel interface or on a physical interface that is configured with a maximum transmission unit (MTU) greater than 4,615 bytes. An attacker could exploit this vulnerability by sending fragmented packets through a VFR-enabled interface on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. | 8.6 | M D |
| CVE-2023-28083 | A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. | 8.3 | M D |
| CVE-2023-28395 | Osprey Pump Controller version 1.01 is vulnerable to a weak session token generation algorithm that can be predicted and can aid in authentication and authorization bypass. This may allow an attacker to hijack a session by predicting the session id and gain unauthorized access to the product. | 8.3 | M D |
| CVE-2023-28597 | Zoom clients prior to 5.13.5 contain an improper trust boundary implementation vulnerability. If a victim saves a local recording to an SMB location and later opens it using a link from Zoom's web portal, an attacker positioned on an adjacent network to the victim client could set up a malicious SMB server to respond to client requests, causing the client to execute attacker controlled executables. This could result in an attacker gaining access to a user's device and data, and remote code execution. | 8.3 | M D |
| CVE-2023-28627 | pymedusa is an automatic video library manager for TV Shows. In versions prior 1.0.12 an attacker with access to the web interface can update the git executable path in /config/general/ > advanced settings with arbitrary OS commands. An attacker may exploit this vulnerability to take execute arbitrary OS commands as the user running the pymedusa program. Users are advised to upgrade. There are no known workarounds for this vulnerability. | 8.3 | M D |
| CVE-2023-28102 | discordrb is an implementation of the Discord API using Ruby. In discordrb before commit `91e13043ffa` the `encoder.rb` file unsafely constructs a shell string using the file parameter, which can potentially leave clients of discordrb vulnerable to command injection. The library is not directly exploitable: the exploit requires that some client of the library calls the vulnerable method with user input. However, if unsafe input reaches the library method, then an attacker can execute arbitrary shell commands on the host machine. Full impact will depend on the permissions of the process running the `discordrb` library and will likely not be total system access. This issue has been addressed in code, but a new release of the `discordrb` gem has not been uploaded to rubygems. This issue is also tracked as `GHSL-2022-094`. | 8.3 | M D |
| CVE-2022-36059 | matrix-js-sdk is a Matrix messaging protocol Client-Server SDK for JavaScript. In versions prior to 19.4.0 events sent with special strings in key places can temporarily disrupt or impede the matrix-js-sdk from functioning properly, potentially impacting the consumer's ability to process data safely. Note that the matrix-js-sdk can appear to be operating normally but be excluding or corrupting runtime data presented to the consumer. This issue has been fixed in matrix-js-sdk 19.4.0 and users are advised to upgrade. Users unable to upgrade may mitigate this issue by redacting applicable events, waiting for the sync processor to store data, and restarting the client. Alternatively, redacting the applicable events and clearing all storage will often fix most perceived issues. In some cases, no workarounds are possible. | 8.2 | M D |
| CVE-2023-28103 | matrix-react-sdk is a Matrix chat protocol SDK for React Javascript. In certain configurations, data sent by remote servers containing special strings in key locations could cause modifications of the `Object.prototype`, disrupting matrix-react-sdk functionality, causing denial of service and potentially affecting program logic. This is fixed in matrix-react-sdk 3.69.0 and users are advised to upgrade. There are no known workarounds for this vulnerability. Note this advisory is distinct from GHSA-2x9c-qwgf-94xr which refers to a similar issue. | 8.2 | M D |
| CVE-2023-28712 | Osprey Pump Controller version 1.01 contains an unauthenticated command injection vulnerability that could allow system access with www-data permissions. | 8.2 | M D |
| CVE-2023-28427 | matrix-js-sdk is a Matrix messaging protocol Client-Server SDK for JavaScript. In versions prior to 24.0.0 events sent with special strings in key places can temporarily disrupt or impede the matrix-js-sdk from functioning properly, potentially impacting the consumer's ability to process data safely. Note that the matrix-js-sdk can appear to be operating normally but be excluding or corrupting runtime data presented to the consumer. This vulnerability is distinct from GHSA-rfv9-x7hh-xc32 which covers a similar issue. The issue has been patched in matrix-js-sdk 24.0.0 and users are advised to upgrade. There are no known workarounds for this vulnerability. | 8.2 | M D |
| CVE-2023-26114 | Versions of the package code-server before 4.10.1 are vulnerable to Missing Origin Validation in WebSockets handshakes. Exploiting this vulnerability can allow an adversary in specific scenarios to access data from and connect to the code-server instance. | 8.2 | M D |
| CVE-2022-36060 | matrix-react-sdk is a Matrix chat protocol SDK for React Javascript. Events sent with special strings in key places can temporarily disrupt or impede the matrix-react-sdk from functioning properly, such as by causing room or event tile crashes. The remainder of the application can appear functional, though certain rooms/events will not be rendered. This issue has been fixed in matrix-react-sdk 3.53.0 and users are advised to upgrade. There are no known workarounds for this vulnerability. | 8.2 | M D |
| CVE-2023-26493 | Cocos Engine is an open-source framework for building 2D & 3D real-time rendering and interactive content. In the github repo for Cocos Engine the `web-interface-check.yml` was subject to command injection. The `web-interface-check.yml` was triggered when a pull request was opened or updated and contained the user controllable field `(${{ github.head_ref }} – the name of the fork's branch)`. This would allow an attacker to take over the GitHub Runner and run custom commands (potentially stealing secrets such as GITHUB_TOKEN) and altering the repository. The workflow has since been removed for the repository. There are no actions required of users. | 8.1 | M D |
| CVE-2023-27700 | MuYuCMS v2.2 was discovered to contain an arbitrary file deletion vulnerability via the component /accessory/picdel.html. | 8.1 | M D |
| CVE-2023-25017 | RIFARTEK IOT Wall has a vulnerability of incorrect authorization. An authenticated remote attacker with general user privilege is allowed to perform specific privileged function to access and modify all sensitive data. | 8.1 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-0870 | A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. | 8.1 | M D |
| CVE-2023-27701 | MuYuCMS v2.2 was discovered to contain an arbitrary file deletion vulnerability via the component /database/sqldel.html. | 8.1 | M D |
| CVE-2023-25195 | Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache Fineract. Authorized users with limited permissions can gain access to server and may be able to use server for any outbound traffic. This issue affects Apache Fineract: from 1.4 through 1.8.3. | 8.1 | M D |
| CVE-2023-0441 | The Gallery Blocks with Lightbox WordPress plugin before 3.0.8 has an AJAX endpoint that can be accessed by any authenticated users, such as subscriber. The callback function allows numerous actions, the most serious one being reading and updating the WordPress options which could be used to enable registration with a default administrator user role. | 8.1 | M D |
| CVE-2023-28441 | smartCARS 3 is flight tracking software. In version 0.5.8 and prior, all persons who have failed login attempts will have their password stored in error logs. This problem doesn't occur in version 0.5.9. As a workaround, delete the affected log file, and ensure one logs in correctly. | 8.0 | M D |
| CVE-2023-25801 | TensorFlow is an open source machine learning platform. Prior to versions 2.12.0 and 2.11.1, `nn_ops.fractional_avg_pool_v2` and `nn_ops.fractional_max_pool_v2` require the first and fourth elements of their parameter `pooling_ratio` to be equal to 1.0, as pooling on batch and channel dimensions is not supported. A fix is included in TensorFlow 2.12.0 and 2.11.1. | 8.0 | M D |
| CVE-2022-24973 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13992. | 8.0 | M D |
| CVE-2023-28637 | DataEase is an open source data visualization analysis tool. In Dataease users are normally allowed to modify data and the data sources are expected to properly sanitize data. The AWS redshift data source does not provide data sanitization which may lead to remote code execution. This vulnerability has been fixed in v1.18.5. Users are advised to upgrade. There are no known workarounds for this vulnerability. | 8.0 | M D |
| CVE-2023-20055 | A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the attacker would need at least valid Observer credentials. | 8.0 | M D |
| CVE-2022-0650 | This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13993. | 8.0 | M D |
| CVE-2023-1516 | RoboDK versions 5.5.3 and prior contain an insecure permission assignment to critical directories vulnerability, which could allow a local user to escalate privileges and write files to the RoboDK process and achieve code execution. | 7.9 | M D |
| CVE-2023-24304 | Improper input validation in the PDF.dll plugin of IrfanView v4.60 allows attackers to execute arbitrary code via opening a crafted PDF file. | 7.8 | M D |
| CVE-2023-25907 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-20911 | In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498 | 7.8 | M D |
| CVE-2023-20917 | In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242605257 | 7.8 | M D |
| CVE-2023-21002 | In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193935 | 7.8 | M D |
| CVE-2023-21024 | In maybeFinish of FallbackHome.java, there is a possible delay of lockdown screen due to logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246543238 | 7.8 | M D |
| CVE-2023-21021 | In isTargetSdkLessThanQOrPrivileged of WifiServiceImpl.java, there is a possible way for the guest user to change admin user network settings due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255537598 | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20931 | In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 | 7.8 | M D |
| CVE-2023-20936 | In bta_av_rc_disc_done of bta_av_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-226927612 | 7.8 | M D |
| CVE-2023-20947 | In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237405974 | 7.8 | M D |
| CVE-2023-21022 | In BufferBlock of Suballocation.cpp, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236098131 | 7.8 | M D |
| CVE-2022-20542 | In parseParamsBlob of types.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238083570 | 7.8 | M D |
| CVE-2023-20906 | In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577 | 7.8 | M D |
| CVE-2023-20955 | In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258653813 | 7.8 | M D |
| CVE-2023-21017 | In InstallStart of InstallStart.java, there is a possible way to change the installer package name due to an improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236687884 | 7.8 | M D |
| CVE-2023-28759 | An issue was discovered in Veritas NetBackup before 10.0 on Windows. A vulnerability in the way the client validates the path to a DLL prior to loading may allow a lower-level user to elevate privileges and compromise the system. | 7.8 | M D |
| CVE-2023-1135 | In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could set incorrect directory permissions, which could result in local privilege escalation. | 7.8 | M D |
| CVE-2022-4095 | A use-after-free flaw was found in Linux kernel before 5.19.2. This issue occurs in cmd_hdl_filter in drivers/staging/rtl8712/rtl8712_cmd.c, allowing an attacker to launch a local denial of service attack and gain escalation of privileges. | 7.8 | M D |
| CVE-2023-21015 | In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244569778 | 7.8 | M D |
| CVE-2023-21005 | In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193946 | 7.8 | M D |
| CVE-2023-26337 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-1281 | Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect hash area can be updated while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tcf_ext. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee059170b1f7e94e55fa6cadee544e176a6e59c2. | 7.8 | M D |
| CVE-2023-26336 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26335 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-1145 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a deserialization vulnerability targeting the Device-DataCollect service, which could allow deserialization of requests prior to authentication, resulting in remote code execution. | 7.8 | M D |
| CVE-2023-1655 | Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.4.0. | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20953 | In onPrimaryClipChanged of ClipboardListener.java, there is a possible way to bypass factory reset protection due to incorrect UI being shown prior to setup completion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251778420 | 7.8 | M D |
| CVE-2023-20957 | In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561 | 7.8 | M D |
| CVE-2023-21001 | In onContextItemSelected of NetworkProviderSettings.java, there is a possible way for users to change the Wi-Fi settings of other users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-237672190 | 7.8 | M D |
| CVE-2023-25861 | Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-0386 | A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system. | 7.8 | M D |
| CVE-2023-21068 | In (TBD) of (TBD), there is a possible way to boot with a hidden debug policy due to a missing warning to the user. This could lead to local escalation of privilege after preparing the device, hiding the warning, and passing the phone to a new user, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243433344References: N/A | 7.8 | M D |
| CVE-2023-1676 | A vulnerability was found in DriverGenius 9.70.0.346. It has been declared as critical. Affected by this vulnerability is the function 0x9C402088 in the library mydrivers64.sys of the component IOCTL Handler. The manipulation leads to memory corruption. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-224233 was assigned to this vulnerability. | 7.8 | M D |
| CVE-2023-1518 | CP Plus KVMS Pro versions 2.01.0.T.190521 and prior are vulnerable to sensitive credentials being leaked because they are insufficiently protected. | 7.8 | M D |
| CVE-2023-20985 | In BTA_GATTS_HandleValueIndication of bta_gatts_api.cc, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245915315 | 7.8 | M D |
| CVE-2023-24308 | A potential memory vulnerability due to insufficient input validation in PDFXEditCore.x64.dll in PDF-XChange Editor version 9.3 by Tracker Software may allow attackers to execute code when a user opens a crafted PDF file. The issue occurs when handling a large number of objects in a PDF file. | 7.8 | M D |
| CVE-2023-20975 | In getAvailabilityStatus of EnableContentCapturePreferenceController.java, there is a possible way to bypass DISALLOW_CONTENT_CAPTURE due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-250573776 | 7.8 | M D |
| CVE-2023-26426 | Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-20995 | In captureImage of CustomizedSensor.cpp, there is a possible way to bypass the fingerprint unlock due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-241910279 | 7.8 | M D |
| CVE-2023-21000 | In MediaCodec.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-194783918 | 7.8 | M D |
| CVE-2023-25590 | A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. | 7.8 | M D |
| CVE-2023-20971 | In removePermission of PermissionManagerServiceImpl.java, there is a possible way to obtain dangerous permissions without user consent due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 7.8 | M D |
| CVE-2023-25860 | Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26088 | In Malwarebytes before 4.5.23, a symbolic link may be used delete any arbitrary file on the system by exploiting the local quarantine system. It can also lead to privilege escalation in certain scenarios. | 7.8 | M D |
| CVE-2023-26334 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-21041 | In append_to_params of param_util.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-250123688References: N/A | 7.8 | M D |
| CVE-2023-21040 | In buildCommand of bluetooth_ccc.cc, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238420277References: N/A | 7.8 | M D |
| CVE-2023-25859 | Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-21035 | In multiple functions of BackupHelper.java, there is a possible way for an app to get permissions previously granted to another app with the same package name due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-184847040 | 7.8 | M D |
| CVE-2023-21034 | In multiple functions of SensorService.cpp, there is a possible access of accurate sensor data due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230358834 | 7.8 | M D |
| CVE-2023-20966 | In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242299736 | 7.8 | M D |
| CVE-2023-21030 | In Confirmation of keystore_cli_v2.cpp, there is a possible way to corrupt memory due to a double free. This could lead to local escalation of privilege in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226234140 | 7.8 | M D |
| CVE-2023-20964 | In multiple functions of MediaSessionRecord.java, there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121 | 7.8 | M D |
| CVE-2023-20963 | In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 | 7.8 | M D |
| CVE-2023-20959 | In AddSupervisedUserActivity, guest users are not prevented from starting the activity due to missing permissions checks. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-249057848 | 7.8 | M D |
| CVE-2023-20993 | In multiple functions of SnoozeHelper.java, there is a possible failure to persist settings due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261588851 | 7.8 | M D |
| CVE-2023-0494 | A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. | 7.8 | M D |
| CVE-2023-21004 | In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193664 | 7.8 | M D |
| CVE-2023-26333 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25880 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25887 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25886 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25885 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25884 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-25883 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25882 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25881 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25879 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-1252 | A use-after-free flaw was found in the Linux kernel's Ext4 File System in how a user triggers several file operations simultaneously with the overlay FS usage. This flaw allows a local user to crash or potentially escalate their privileges on the system. Only if patch 9a2544037600 ("ovl: fix use after free in struct ovl_aio_req") not applied yet, the kernel could be affected. | 7.8 | M D |
| CVE-2022-24908 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. Crafted data in a JP2 image can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16187. | 7.8 | M D |
| CVE-2022-24907 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. Crafted data in a JP2 image can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16186. | 7.8 | M D |
| CVE-2023-26327 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26328 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26329 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26330 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2022-1229 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.2.034. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of IFC files. Crafted data in an IFC file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16581. | 7.8 | M D |
| CVE-2023-25888 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25889 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25890 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25891 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25906 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25905 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-25904 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25903 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25902 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25901 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25900 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25899 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25898 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25897 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25896 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25895 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25894 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25893 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25892 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26332 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-26331 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25874 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-20065 | A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. | 7.8 | M D |
| CVE-2023-25864 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25867 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-25868 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25869 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25870 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25871 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25872 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25873 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25908 | Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-28596 | Zoom Client for IT Admin macOS installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability in an attack chain during the installation process to escalate their privileges to privileges to root. | 7.8 | M D |
| CVE-2023-25863 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-25866 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2023-20035 | A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. | 7.8 | M D |
| CVE-2023-1078 | A flaw was found in the Linux Kernel in RDS (Reliable Datagram Sockets) protocol. The rds_rm_zerocopy_callback() uses list_entry() on the head of a list causing a type confusion. Local user can trigger this with rds_message_put(). Type confusion leads to `struct rds_msg_zcopy_info *info` actually points to something else that is potentially controlled by local user. It is known how to trigger this, which causes an out of bounds access, and a lock corruption. | 7.8 | M D |
| CVE-2023-21003 | In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193711 | 7.8 | M D |
| CVE-2021-3674 | A flaw was found in rizin. The create_section_from_phdr function allocates space for ELF section data by processing the headers. Crafted values in the headers can cause out of bounds reads, which can lead to memory corruption and possibly code execution through the binary object's callback function. | 7.8 | M D |
| CVE-2022-47502 | Apache OpenOffice documents can contain links that call internal macros with arbitrary arguments. Several URI Schemes are defined for this purpose. Links can be activated by clicks, or by automatic document events. The execution of such links must be subject to user approval. In the affected versions of OpenOffice, approval for certain links is not requested; when activated, such links could therefore result in arbitrary script execution. | 7.8 | M D |
| CVE-2023-0179 | A buffer overflow vulnerability was found in the Netfilter subsystem in the Linux Kernel. This issue could allow the leakage of both stack and heap addresses, and potentially allow Local Privilege Escalation to the root user via arbitrary code execution. | 7.8 | M D |
| CVE-2022-38745 | Apache OpenOffice versions before 4.1.14 may be configured to add an empty entry to the Java class path. This may lead to run arbitrary Java code from the current directory. | 7.8 | M D |
| CVE-2023-1654 | Denial of Service in GitHub repository gpac/gpac prior to 2.4.0. | 7.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-26547 | The InputMethod module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation. | 7.8 | M D |
| CVE-2023-24295 | A stack overfow in SoftMaker Software GmbH FlexiPDF v3.0.3.0 allows attackers to execute arbitrary code after opening a crafted PDF file. | 7.8 | M D |
| CVE-2023-1399 | N6854A Geolocation Server versions 2.4.2 are vulnerable to untrusted data deserialization, which may allow a malicious actor to escalate privileges in the affected device's default configuration and achieve remote code execution. | 7.8 | M D |
| CVE-2023-25865 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | M D |
| CVE-2022-3683 | A vulnerability exists in the SDM600 API web services authorization validation implementation. An attacker who successfully exploits the vulnerability could read data directly from a data store that is not restricted, or insufficiently protected, having access to sensitive data. This issue affects: All SDM600 versions prior to version 1.2 FP3 HF4 (Build Nr. 1.2.23000.291) List of CPEs: * cpe:2.3:a:hitachienergy:sdm600:1.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.1:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.9002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.10002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.11002.149:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.12002.222:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.13002.72:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.44:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.92:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.108:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.182:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.342:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.447:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.481:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.506:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.566:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.20000.3174:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.291:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.931:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.105:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.23000.291:*:*:*:*:*:*:* | 7.7 | M D |
| CVE-2023-25591 | A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. | 7.6 | M D |
| CVE-2023-28117 | Sentry SDK is the official Python SDK for Sentry, real-time crash reporting software. When using the Django integration of versions prior to 1.14.0 of the Sentry SDK in a specific configuration it is possible to leak sensitive cookies values, including the session cookie to Sentry. These sensitive cookies could then be used by someone with access to your Sentry issues to impersonate or escalate their privileges within your application. In order for these sensitive values to be leaked, the Sentry SDK configuration must have `sendDefaultPII` set to `True`; one must use a custom name for either `SESSION_COOKIE_NAME` or `CSRF_COOKIE_NAME` in one's Django settings; and one must not be configured in one's organization or project settings to use Sentry's data scrubbing features to account for the custom cookie names. As of version 1.14.0, the Django integration of the `sentry-sdk` will detect the custom cookie names based on one's Django settings and will remove the values from the payload before sending the data to Sentry. As a workaround, use the SDK's filtering mechanism to remove the cookies from the payload that is sent to Sentry. For error events, this can be done with the `before_send` callback method and for performance related events (transactions) one can use the `before_send_transaction` callback method. Those who want to handle filtering of these values on the server-side can also use Sentry's advanced data scrubbing feature to account for the custom cookie names. Look for the `$http.cookies`, `$http.headers`, `$request.cookies`, or `$request.headers` fields to target with a scrubbing rule. | 7.6 | M D |
| CVE-2021-43315 | A heap-based buffer overflows was discovered in upx, during the generic pointer 'p' points to an inaccessible address in func get_le32(). The problem is essentially caused in PackLinuxElf32::elf_lookup() at p_lx_elf.cpp:5349 | 7.5 | M D |
| CVE-2022-46397 | FP.io VPP (Vector Packet Processor) 22.10, 22.06, 22.02, 21.10, 21.06, 21.01, 20.09, 20.05, 20.01, 19.08, and 19.04 Generates a Predictable IV with CBC Mode. | 7.5 | M D |
| CVE-2021-43316 | A heap-based buffer overflow was discovered in upx, during the generic pointer 'p' points to an inaccessible address in func get_le64(). | 7.5 | M D |
| CVE-2021-43317 | A heap-based buffer overflows was discovered in upx, during the generic pointer 'p' points to an inaccessible address in func get_le32(). The problem is essentially caused in PackLinuxElf64::elf_lookup() at p_lx_elf.cpp:5404 | 7.5 | M D |
| CVE-2021-43314 | A heap-based buffer overflows was discovered in upx, during the generic pointer 'p' points to an inaccessible address in func get_le32(). The problem is essentially caused in PackLinuxElf32::elf_lookup() at p_lx_elf.cpp:5368 | 7.5 | M D |
| CVE-2021-43313 | A heap-based buffer overflow was discovered in upx, during the variable 'bucket' points to an inaccessible address. The issue is being triggered in the function PackLinuxElf32::invert_pt_dynamic at p_lx_elf.cpp:1688. | 7.5 | M D |
| CVE-2023-28375 | Osprey Pump Controller version 1.01 is vulnerable to an unauthenticated file disclosure. Using a GET parameter, attackers can disclose arbitrary files on the affected device and disclose sensitive and system information. | 7.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2021-43312 | A heap-based buffer overflow was discovered in upx, during the variable 'bucket' points to an inaccessible address. The issue is being triggered in the function PackLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5239. | 7.5 | M D |
| CVE-2021-43311 | A heap-based buffer overflow was discovered in upx, during the generic pointer 'p' points to an inaccessible address in func get_le32(). The problem is essentially caused in PackLinuxElf32::elf_lookup() at p_lx_elf.cpp:5382. | 7.5 | M D |
| CVE-2023-28442 | GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the `/geoserver/rest/about/status` Geoserver REST API endpoint. The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration is provided by `geoserver-geonode-ext`. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing `<geoserver_datadir>/security/rest.properties` file. | 7.5 | M D |
| CVE-2023-28648 | Osprey Pump Controller version 1.01 inputs passed to a GET parameter are not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML/JS code in a user's browser session in context of an affected site. | 7.5 | M D |
| CVE-2023-26071 | An issue was discovered in MCUBO ICT through 10.12.4 (aka 6.0.2). An Observable Response Discrepancy can occur under the login web page. In particular, the web application provides different responses to incoming requests in a way that reveals internal state information to an unauthorized actor. That allow an unauthorized actor to perform User Enumeration attacks. | 7.5 | M D |
| CVE-2023-27579 | TensorFlow is an end-to-end open source platform for machine learning. Constructing a tflite model with a paramater `filter_input_channel` of less than 1 gives a FPE. This issue has been patched in version 2.12. TensorFlow will also cherrypick the fix commit on TensorFlow 2.11.1. | 7.5 | M D |
| CVE-2023-21027 | In multiple functions of PasspointXmlUtils.java, there is a possible authentication misconfiguration due to a logic error in the code. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-216854451 | 7.5 | M D |
| CVE-2022-48357 | Some products have the double fetch vulnerability. Successful exploitation of this vulnerability may cause denial of service (DoS) attacks to the kernel. | 7.5 | M D |
| CVE-2023-1138 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain an improper access control vulnerability, which could allow an attacker to retrieve Gateway configuration files to obtain plaintext credentials. | 7.5 | M D |
| CVE-2023-1142 | In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could use URL decoding to retrieve system files, credentials, and bypass authentication resulting in privilege escalation. | 7.5 | M D |
| CVE-2023-22247 | Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and earlier) are affected by an XML Injection vulnerability that could lead to arbitrary file system read. An unauthenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction. | 7.5 | M D |
| CVE-2022-3116 | The Heimdal Software Kerberos 5 implementation is vulnerable to a null pointer dereferance. An attacker with network access to an application that depends on the vulnerable code path can cause the application to crash. | 7.5 | M D |
| CVE-2022-48346 | The HwContacts module has a logic bypass vulnerability. Successful exploitation of this vulnerability may affect confidentiality. | 7.5 | M D |
| CVE-2022-48347 | The MediaProvider module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect confidentiality. | 7.5 | M D |
| CVE-2022-48350 | The HUAWEI Messaging app has a vulnerability of unauthorized file access. Successful exploitation of this vulnerability may affect confidentiality. | 7.5 | M D |
| CVE-2022-48351 | The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect availability. | 7.5 | M D |
| CVE-2022-48352 | Some smartphones have data initialization issues. Successful exploitation of this vulnerability may cause a system panic. | 7.5 | M D |
| CVE-2022-48356 | The facial recognition module has a vulnerability in input parameter verification. Successful exploitation of this vulnerability may cause failed facial recognition. | 7.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-48359 | The recovery mode for updates has a vulnerability that causes arbitrary disk modification. Successful exploitation of this vulnerability may affect confidentiality. | 7.5 | M D |
| CVE-2023-21028 | In parse_printerAttributes of ipphelper.c, there is a possible out of bounds read due to a string without a null-terminator. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-180680572 | 7.5 | M D |
| CVE-2022-48360 | The facial recognition module has a vulnerability in file permission control. Successful exploitation of this vulnerability may affect confidentiality. | 7.5 | M D |
| CVE-2023-0210 | A bug affects the Linux kernel's ksmbd NTLMv2 authentication and is known to crash the OS immediately in Linux-based systems. | 7.5 | M D |
| CVE-2023-20860 | Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass. | 7.5 | M D |
| CVE-2023-26548 | The pgmng module has a vulnerability in serialization/deserialization. Successful exploitation of this vulnerability may affect availability. | 7.5 | M D |
| CVE-2023-26549 | The SystemUI module has a vulnerability of repeated app restart due to improper parameters. Successful exploitation of this vulnerability may affect confidentiality. | 7.5 | M D |
| CVE-2023-23330 | amano Xparc parking solutions 7.1.3879 was discovered to be vulnerable to local file inclusion. | 7.5 | M D |
| CVE-2023-25262 | Stimulsoft GmbH Stimulsoft Designer (Web) 2023.1.3 is vulnerable to Server Side Request Forgery (SSRF). TThe Reporting Designer (Web) offers the possibility to embed sources from external locations. If the user chooses an external location, the request to that resource is performed by the server rather than the client. Therefore, the server causes outbound traffic and potentially imports data. An attacker may also leverage this behaviour to exfiltrate data of machines on the internal network of the server hosting the Stimulsoft Reporting Designer (Web). | 7.5 | M D |
| CVE-2022-3684 | A vulnerability exists in a SDM600 endpoint. An attacker could exploit this vulnerability by running multiple parallel requests, the SDM600 web services become busy rendering the application unresponsive. This issue affects: All SDM600 versions prior to version 1.2 FP3 HF4 (Build Nr. 1.2.23000.291) List of CPEs: * cpe:2.3:a:hitachienergy:sdm600:1.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.1:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.9002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.10002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.11002.149:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.12002.222:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.13002.72:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.44:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.92:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.108:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.182:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.342:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.447:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.481:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.506:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.566:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.20000.3174:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.291:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.931:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.105:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.23000.291:*:*:*:*:*:*:* | 7.5 | M D |
| CVE-2022-3685 | A vulnerability exists in the SDM600 software. The software operates at a privilege level that is higher than the minimum level required. An attacker who successfully exploits this vulnerability can escalate privileges. This issue affects: All SDM600 versions prior to version 1.3.0. List of CPEs: * cpe:2.3:a:hitachienergy:sdm600:1.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.1:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.9002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.10002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.11002.149:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.12002.222:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.13002.72:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.44:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.92:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.108:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.182:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.342:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.447:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.481:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.506:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.566:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.20000.3174:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.291:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.931:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.105:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.23000.291:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.3.0.1339:*:*:*:*:*:*:* | 7.5 | M D |
| CVE-2023-25260 | Stimulsoft Designer (Web) 2023.1.3 is vulnerable to Local File Inclusion. | 7.5 | M D |
| CVE-2023-24094 | An issue in the bridge2 component of MikroTik RouterOS v6.40.5 allows attackers to cause a Denial of Service (DoS) via crafted packets. | 7.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-47925 | The validate JSON endpoint of the Secvisogram csaf-validator-service in versions < 0.1.0 processes tests with unexpected names. This insufficient input validation of requests by an unauthenticated remote user might lead to a partial DoS of the service. Only the request of the attacker is affected by this vulnerability. | 7.5 | M D |
| CVE-2020-8889 | The ShipStation.com plugin 1.0 for CS-Cart allows remote attackers to obtain sensitive information (via action=export) because a typo results in a successful comparison of a blank password and NULL. | 7.5 | M D |
| CVE-2023-28867 | In GraphQL Java (aka graphql-java) before 20.1, an attacker can send a crafted GraphQL query that causes stack consumption. The fixed versions are 20.1, 19.4, 18.4, 17.5, and 0.0.0-2023-03-20T01-49-44-80e3135. | 7.5 | M D |
| CVE-2023-21053 | In sms_ExtractCbLanguage of sms_CellBroadcast.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-251805610References: N/A | 7.5 | M D |
| CVE-2023-21060 | In sms_GetTpPiIe of sms_PduCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253770924References: N/A | 7.5 | M D |
| CVE-2023-21061 | Product: AndroidVersions: Android kernelAndroid ID: A-229255400References: N/A | 7.5 | M D |
| CVE-2023-21067 | Product: AndroidVersions: Android kernelAndroid ID: A-254114726References: N/A | 7.5 | M D |
| CVE-2023-27055 | Aver Information Inc PTZApp2 v20.01044.48 allows attackers to access sensitive files via a crafted GET request. | 7.5 | M D |
| CVE-2023-25658 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, an out of bounds read is in GRUBlockCellGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. | 7.5 | M D |
| CVE-2023-25659 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the parameter `indices` for `DynamicStitch` does not match the shape of the parameter `data`, it can trigger an stack OOB read. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25660 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when the parameter `summarize` of `tf.raw_ops.Print` is zero, the new method `SummarizeArray<bool>` will reference to a nullptr, leading to a seg fault. A fix is included in TensorFlow version 2.12 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25662 | TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 are vulnerable to integer overflow in EditDistance. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25663 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `ctx->step_containter()` is a null ptr, the Lookup function will be executed with a null pointer. A fix is included in TensorFlow 2.12.0 and 2.11.1. | 7.5 | M D |
| CVE-2023-25664 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAvgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. | 7.5 | M D |
| CVE-2023-25665 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `SparseSparseMaximum` is given invalid sparse tensors as inputs, it can give a null pointer error. A fix is included in TensorFlow version 2.12 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25666 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a floating point exception in AudioSpectrogram. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25669 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the stride and window size are not positive for `tf.raw_ops.AvgPoolGrad`, it can give a floating point exception. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25670 | TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 have a null point error in QuantizedMatMulWithBiasAndDequantize with MKL enabled. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25671 | TensorFlow is an open source platform for machine learning. There is out-of-bounds access due to mismatched integer type sizes. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-25672 | TensorFlow is an open source platform for machine learning. The function `tf.raw_ops.LookupTableImportV2` cannot handle scalars in the `values` parameter and gives an NPE. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25673 | TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 have a Floating Point Exception in TensorListSplit with XLA. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 7.5 | M D |
| CVE-2023-25674 | TensorFlow is an open source machine learning platform. Versions prior to 2.12.0 and 2.11.1 have a null pointer error in RandomShuffle with XLA enabled. A fix is included in TensorFlow 2.12.0 and 2.11.1. | 7.5 | M D |
| CVE-2023-25675 | TensorFlow is an open source machine learning platform. When running versions prior to 2.12.0 and 2.11.1 with XLA, `tf.raw_ops.Bincount` segfaults when given a parameter `weights` that is neither the same shape as parameter `arr` nor a length-0 tensor. A fix is included in TensorFlow 2.12.0 and 2.11.1. | 7.5 | M D |
| CVE-2023-25676 | TensorFlow is an open source machine learning platform. When running versions prior to 2.12.0 and 2.11.1 with XLA, `tf.raw_ops.ParallelConcat` segfaults with a nullptr dereference when given a parameter `shape` with rank that is not greater than zero. A fix is available in TensorFlow 2.12.0 and 2.11.1. | 7.5 | M D |
| CVE-2023-27856 | In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. | 7.5 | M D |
| CVE-2023-21059 | In EUTRAN_LCS_DecodeFacilityInformationElement of LPP_LcsManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-247564044References: N/A | 7.5 | M D |
| CVE-2022-45003 | Gophish through 0.12.1 allows attackers to cause a Denial of Service (DoS) via a crafted payload involving autofocus. | 7.5 | M D |
| CVE-2023-28431 | Frontier is an Ethereum compatibility layer for Substrate. Frontier's `modexp` precompile uses `num-bigint` crate under the hood. In the implementation prior to pull request 1017, the cases for modulus being even and modulus being odd are treated separately. Odd modulus uses the fast Montgomery multiplication, and even modulus uses the slow plain power algorithm. This gas cost discrepancy was not accounted for in the `modexp` precompile, leading to possible denial of service attacks. No fixes for `num-bigint` are currently available, and thus this issue is fixed in the short term by raising the gas costs for even modulus, and in the long term fixing it in `num-bigint` or switching to another modexp implementation. The short-term fix for Frontier is deployed at pull request 1017. There are no known workarounds aside from applying the fix. | 7.5 | M D |
| CVE-2023-1370 | [Json-smart](https://netplex.github.io/json-smart/) is a performance focused, JSON processor lib. When reaching a '[' or '{' character in the JSON input, the code parses an array or an object respectively. It was discovered that the code does not have any limit to the nesting of such arrays or objects. Since the parsing of nested arrays and objects is done recursively, nesting too many of them can cause a stack exhaustion (stack overflow) and crash the software. | 7.5 | M D |
| CVE-2023-27077 | Stack Overflow vulnerability found in 360 D901 allows a remote attacker to cause a Distributed Denial of Service (DDOS) via a crafted HTTP package. | 7.5 | M D |
| CVE-2023-20107 | A vulnerability in the deterministic random bit generator (DRBG), also known as pseudorandom number generator (PRNG), in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco ASA 5506-X, ASA 5508-X, and ASA 5516-X Firewalls could allow an unauthenticated, remote attacker to cause a cryptographic collision, enabling the attacker to discover the private key of an affected device. This vulnerability is due to insufficient entropy in the DRBG for the affected hardware platforms when generating cryptographic keys. An attacker could exploit this vulnerability by generating a large number of cryptographic keys on an affected device and looking for collisions with target devices. A successful exploit could allow the attacker to impersonate an affected target device or to decrypt traffic secured by an affected key that is sent to or from an affected target device. | 7.5 | M D |
| CVE-2023-1605 | Denial of Service in GitHub repository radareorg/radare2 prior to 5.8.6. | 7.5 | M D |
| CVE-2023-27079 | Command Injection vulnerability found in Tenda G103 v.1.0.05 allows an attacker to obtain sensitive information via a crafted package | 7.5 | M D |
| CVE-2023-0464 | A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. | 7.5 | M D |
| CVE-2023-28119 | The crewjam/saml go library contains a partial implementation of the SAML standard in golang. Prior to version 0.4.13, the package's use of `flate.NewReader` does not limit the size of the input. The user can pass more than 1 MB of data in the HTTP request to the processing functions, which will be decompressed server-side using the Deflate algorithm. Therefore, after repeating the same request multiple times, it is possible to achieve a reliable crash since the operating system kills the process. This issue is patched in version 0.4.13. | 7.5 | M D |
| CVE-2023-27857 | In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer.  An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. | 7.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-28432 | Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z. | 7.5 | M D |
| CVE-2023-20067 | A vulnerability in the HTTP-based client profiling feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of received traffic. An attacker could exploit this vulnerability by sending crafted traffic through a wireless access point. A successful exploit could allow the attacker to cause CPU utilization to increase, which could result in a DoS condition on an affected device and could cause new wireless client associations to fail. Once the offending traffic stops, the affected system will return to an operational state and new client associations will succeed. | 7.4 | M D |
| CVE-2023-20112 | A vulnerability in Cisco access point (AP) software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of certain parameters within 802.11 frames. An attacker could exploit this vulnerability by sending a wireless 802.11 association request frame with crafted parameters to an affected device. A successful exploit could allow the attacker to cause an unexpected reload of an affected device, resulting in a DoS condition. | 7.4 | M D |
| CVE-2022-48358 | The BatteryHealthActivity has a redirection vulnerability. Successful exploitation of this vulnerability by a malicious app can cause service exceptions. | 7.4 | M D |
| CVE-2023-22812 | SanDisk PrivateAccess versions prior to 6.4.9 support insecure TLS 1.0 and TLS 1.1 protocols which are susceptible to man-in-the-middle attacks thereby compromising confidentiality and integrity of data. | 7.4 | M D |
| CVE-2023-1674 | A vulnerability was found in SourceCodester School Registration and Fee System 1.0 and classified as critical. This issue affects some unknown processing of the file /bilal final/login.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224231. | 7.3 | M D |
| CVE-2023-28430 | OneSignal is an email, sms, push notification, and in-app message service for mobile apps.The Zapier.yml workflow is triggered on issues (types: [closed]) (i.e., when an Issue is closed). The workflow starts with full write-permissions GitHub repository token since the default workflow permissions on Organization/Repository level are set to read-write. This workflow runs the following step with data controlled by the comment `(${{ github.event.issue.title }} – the full title of the Issue)`, allowing an attacker to take over the GitHub Runner and run custom commands, potentially stealing any secret (if used), or altering the repository. This issue was found with CodeQL using javascript's Expression injection in Actions query. This issue has been addressed in the repositories github action. No actions are required by users. This issue is also tracked as `GHSL-2023-051`. | 7.3 | M D |
| CVE-2023-1594 | A vulnerability, which was classified as critical, was found in novel-plus 3.6.2. Affected is the function MenuService of the file sys/menu/list. The manipulation of the argument sort leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223662 is the identifier assigned to this vulnerability. | 7.3 | M D |
| CVE-2023-20976 | In getConfirmationMessage of DefaultAutofillPicker.java, there is a possible way to mislead the user to select default autofill application due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-216117246 | 7.3 | M D |
| CVE-2023-24835 | Softnext Technologies Corp.'s SPAM SQR has a vulnerability of Code Injection within its specific function. An authenticated remote attacker with administrator privilege can exploit this vulnerability to execute arbitrary system command to perform arbitrary system operation or disrupt service. | 7.2 | M D |
| CVE-2023-1168 | An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. | 7.2 | M D |
| CVE-2023-1458 | A vulnerability has been found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6 and classified as critical. Affected by this vulnerability is an unknown functionality of the component OSPF Handler. The manipulation of the argument area leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The associated identifier of this vulnerability is VDB-223303. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. | 7.2 | M D |
| CVE-2023-24840 | HGiga MailSherlock mail query function has vulnerability of insufficient validation for user input. An authenticated remote attacker with administrator privilege can exploit this vulnerability to inject SQL commands to read, modify, and delete the database. | 7.2 | M D |
| CVE-2023-1456 | A vulnerability, which was classified as critical, has been found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. This issue affects some unknown processing of the component NAT Configuration Handler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier VDB-223301 was assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. | 7.2 | M D |
| CVE-2022-30037 | XunRuiCMS v4.3.3 to v4.5.1 vulnerable to PHP file write and CMS PHP file inclusion, allows attackers to execute arbitrary php code, via the add function in cron.php. | 7.2 | M D |
| CVE-2023-1457 | A vulnerability, which was classified as critical, was found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. Affected is an unknown function of the component Static Routing Configuration Handler. The manipulation of the argument next-hop-interface 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 real existence of this vulnerability is still doubted at the moment. VDB-223302 is the identifier assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. | 7.2 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-25828 | Pluck CMS is vulnerable to an authenticated remote code execution (RCE) vulnerability through its “albums” module. Albums are used to create collections of images that can be inserted into web pages across the site. Albums allow the upload of various filetypes, which undergo a normalization process before being available on the site. Due to lack of file extension validation, it is possible to upload a crafted JPEG payload containing an embedded PHP web-shell. An attacker may navigate to it directly to achieve RCE on the underlying web server. Administrator credentials for the Pluck CMS web interface are required to access the albums module feature, and are thus required to exploit this vulnerability. CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C (8.2 High) | 7.2 | M D |
| CVE-2023-23192 | IS Decisions UserLock MFA 11.01 is vulnerable to authentication bypass using scheduled task. | 7.2 | M D |
| CVE-2023-21054 | In EUTRAN_LCS_ConvertLCS_MOLRReq of LPP_CommonUtil.c, there is a possible out of bounds write due to a logic error in the code. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244556535References: N/A | 7.2 | M D |
| CVE-2023-24841 | HGiga MailSherlock query function for connection log has a vulnerability of insufficient filtering for user input. An authenticated remote attacker with administrator privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operation or disrupt service. | 7.2 | M D |
| CVE-2022-47145 | Reflected Cross-Site Scripting (XSS) vulnerability in Blockonomics WordPress Bitcoin Payments – Blockonomics plugin <= 3.5.7 versions. | 7.1 | M D |
| CVE-2023-28758 | An issue was discovered in Veritas NetBackup before 8.3.0.2. BPCD allows an unprivileged user to specify a log file path when executing a NetBackup command. This can be used to overwrite existing NetBackup log files. | 7.1 | M D |
| CVE-2023-25593 | Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. | 7.1 | M D |
| CVE-2023-1134 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a path traversal vulnerability, which could allow an attacker to read local files, disclose plaintext credentials, and escalate privileges. | 7.1 | M D |
| CVE-2023-20958 | In read_paint of ttcolr.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254803162 | 7.1 | M D |
| CVE-2022-47146 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Contempoinc Real Estate 7 WordPress theme <= 3.3.1 versions. | 7.1 | M D |
| CVE-2023-22704 | Reflected Cross-Site Scripting (XSS) vulnerability in Michael Winkler teachPress plugin <= 8.1.8 versions. | 7.1 | M D |
| CVE-2022-46843 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Le Van Toan Woocommerce Vietnam Checkout plugin <= 2.0.4 versions. | 7.1 | M D |
| CVE-2023-28685 | Jenkins AbsInt a³ Plugin 1.1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. | 7.1 | M D |
| CVE-2022-47431 | Reflected Cross-Site Scripting (XSS) vulnerability in Tussendoor internet & marketing Open RDW kenteken voertuiginformatie plugin <= 2.0.14 versions. | 7.1 | M D |
| CVE-2023-25592 | Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. | 7.1 | M D |
| CVE-2023-28686 | Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. | 7.1 | M D |
| CVE-2023-28718 | Osprey Pump Controller version 1.01 allows users to perform certain actions via HTTP requests without performing any checks to verify the requests. This may allow an attacker to perform certain actions with administrative privileges if a logged-in user visits a malicious website. | 7.1 | M D |
| CVE-2023-1380 | A slab-out-of-bound read problem was found in brcmf_get_assoc_ies in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux Kernel. This issue could occur when assoc_info->req_len data is bigger than the size of the buffer, defined as WL_EXTRA_BUF_MAX, leading to a denial of service. | 7.1 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-28447 | Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability. | 7.1 | M D |
| CVE-2022-45831 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in biplob018 Image Hover Effects for Elementor with Lightbox and Flipbox plugin <= 2.8 versions. | 7.1 | M D |
| CVE-2022-45825 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in iThemes WPComplete plugin <= 2.9.2 versions. | 7.1 | M D |
| CVE-2023-1077 | In the Linux kernel, pick_next_rt_entity() may return a type confused entry, not detected by the BUG_ON condition, as the confused entry will not be NULL, but list_head.The buggy error condition would lead to a type confused entry with the list head,which would then be used as a type confused sched_rt_entity,causing memory corruption. | 7.0 | M D |
| CVE-2023-28638 | Snappier is a high performance C# implementation of the Snappy compression algorithm. This is a buffer overrun vulnerability that can affect any user of Snappier 1.1.0. In this release, much of the code was rewritten to use byte references rather than pointers to pinned buffers. This change generally improves performance and reduces workload on the garbage collector. However, when the garbage collector performs compaction and rearranges memory, it must update any byte references on the stack to refer to the updated location. The .NET garbage collector can only update these byte references if they still point within the buffer or to a point one byte past the end of the buffer. If they point outside this area, the buffer itself may be moved while the byte reference stays the same. There are several places in 1.1.0 where byte references very briefly point outside the valid areas of buffers. These are at locations in the code being used for buffer range checks. While the invalid references are never dereferenced directly, if a GC compaction were to occur during the brief window when they are on the stack then it could invalidate the buffer range check and allow other operations to overrun the buffer. This should be very difficult for an attacker to trigger intentionally. It would require a repetitive bulk attack with the hope that a GC compaction would occur at precisely the right moment during one of the requests. However, one of the range checks with this problem is a check based on input data in the decompression buffer, meaning malformed input data could be used to increase the chance of success. Note that any resulting buffer overrun is likely to cause access to protected memory, which will then cause an exception and the process to be terminated. Therefore, the most likely result of an attack is a denial of service. This issue has been patched in release 1.1.1. Users are advised to upgrade. Users unable to upgrade may pin buffers to a fixed location before using them for compression or decompression to mitigate some, but not all, of these cases. At least one temporary decompression buffer is internal to the library and never pinned. | 7.0 | M D |
| CVE-2023-26923 | Musescore 3.0 to 4.0.1 has a stack buffer overflow vulnerability that occurs when reading misconfigured midi files. If attacker can additional information, attacker can execute arbitrary code. | 7.0 | M D |
| CVE-2023-28005 | A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows® Secure Boot process in an attempt to execute other attacks to obtain access to the contents of the device. An attacker must first obtain physical access to the target system in order to exploit this vulnerability. It is also important to note that the contents of the drive(s) encrypted with TMEE FDE would still be protected and would NOT be accessible by the attacker by exploitation of this vulnerability alone. | 6.8 | M D |
| CVE-2023-1079 | A flaw was found in the Linux kernel. A use-after-free may be triggered in asus_kbd_backlight_set when plugging/disconnecting in a malicious USB device, which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, the work_struct may be scheduled by the LED controller while the device is disconnecting, triggering a use-after-free on the struct asus_kbd_leds *led structure. A malicious USB device may exploit the issue to cause memory corruption with controlled data. | 6.8 | M D |
| CVE-2023-20926 | In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 | 6.8 | M D |
| CVE-2023-20100 | A vulnerability in the access point (AP) joining process of the Control and Provisioning of Wireless Access Points (CAPWAP) protocol of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a logic error that occurs when certain conditions are met during the AP joining process. An attacker could exploit this vulnerability by adding an AP that is under their control to the network. The attacker then must ensure that the AP successfully joins an affected wireless controller under certain conditions. Additionally, the attacker would need the ability to restart a valid AP that was previously connected to the controller. A successful exploit could allow the attacker to cause the affected device to restart unexpectedly, resulting in a DoS condition. | 6.8 | M D |
| CVE-2023-28885 | The MyLink infotainment system (build 2021.3.26) in General Motors Chevrolet Equinox 2021 vehicles allows attackers to cause a denial of service (temporary failure of Media Player functionality) via a crafted MP3 file. | 6.8 | M D |
| CVE-2023-0778 | A Time-of-check Time-of-use (TOCTOU) flaw was found in podman. This issue may allow a malicious user to replace a normal file in a volume with a symlink while exporting the volume, allowing for access to arbitrary files on the host file system. | 6.8 | M D |
| CVE-2023-20081 | A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. | 6.8 | M D |
| CVE-2023-21062 | In DoSetTempEcc of imsservice.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243376770References: N/A | 6.7 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-21076 | In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A | 6.7 | M D |
| CVE-2023-21042 | In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239873326References: N/A | 6.7 | M D |
| CVE-2023-21043 | In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239872581References: N/A | 6.7 | M D |
| CVE-2023-21050 | In load_png_image of ExynosHWCHelper.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244423702References: N/A | 6.7 | M D |
| CVE-2023-21051 | In dwc3_exynos_clk_get of dwc3-exynos.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323322References: N/A | 6.7 | M D |
| CVE-2022-47529 | Insecure Win32 memory objects in Endpoint Windows Agents in RSA NetWitness Platform before 12.2 allow local and admin Windows user accounts to modify the endpoint agent service configuration: to either disable it completely or run user-supplied code or commands, thereby bypassing tamper-protection features via ACL modification. | 6.7 | M D |
| CVE-2023-20994 | In _ufdt_output_property_to_fdt of ufdt_convert.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259062118 | 6.7 | M D |
| CVE-2023-21079 | In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254839721References: N/A | 6.7 | M D |
| CVE-2023-21078 | In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254840211References: N/A | 6.7 | M D |
| CVE-2023-21077 | In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257289560References: N/A | 6.7 | M D |
| CVE-2023-21075 | In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A | 6.7 | M D |
| CVE-2023-21063 | In ParseWithAuthType of simdata.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243129862References: N/A | 6.7 | M D |
| CVE-2023-21020 | In registerSignalHandlers of main.c, there is a possible local arbitrary code execution due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256591441 | 6.7 | M D |
| CVE-2023-21073 | In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A | 6.7 | M D |
| CVE-2023-21072 | In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A | 6.7 | M D |
| CVE-2023-21071 | In dhd_prot_ioctcmplt_process of dhd_msgbuf.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028518References: N/A | 6.7 | M D |
| CVE-2023-21052 | In setToExternal of ril_external_client.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259063189References: N/A | 6.7 | M D |
| CVE-2023-21070 | In add_roam_cache_list of wl_roam.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028776References: N/A | 6.7 | M D |
| CVE-2023-21018 | In UnwindingWorker of unwinding.cc, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233338564 | 6.7 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-21056 | In lwis_slc_buffer_free of lwis_device_slc.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-245300559References: N/A | 6.7 | M D |
| CVE-2023-21065 | In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239630493References: N/A | 6.7 | M D |
| CVE-2023-21064 | In DoSetPinControl of miscservice.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243130078References: N/A | 6.7 | M D |
| CVE-2023-21069 | In wl_update_hidden_ap_ie of wl_cfgscan.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254029309References: N/A | 6.7 | M D |
| CVE-2023-21038 | In cs40l2x_cp_trigger_queue_show of cs40l2x.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-224000736References: N/A | 6.7 | M D |
| CVE-2022-43863 | IBM QRadar SIEM 7.4 and 7.5 is vulnerable to privilege escalation, allowing a user with some admin capabilities to gain additional admin capabilities. IBM X-Force ID: 239425. | 6.7 | M D |
| CVE-2023-28772 | An issue was discovered in the Linux kernel before 5.13.3. lib/seq_buf.c has a seq_buf_putmem_hex buffer overflow. | 6.7 | M D |
| CVE-2022-42500 | In OEM_OnRequest of sced.cpp, there is a possible shell command execution due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239701389References: N/A | 6.7 | M D |
| CVE-2023-1073 | A memory corruption flaw was found in the Linux kernel's human interface device (HID) subsystem in how a user inserts a malicious USB device. This flaw allows a local user to crash or potentially escalate their privileges on the system. | 6.6 | M D |
| CVE-2023-1137 | Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability in which a low-level user could extract files and plaintext credentials of administrator users, resulting in privilege escalation. | 6.5 | M D |
| CVE-2023-0241 | pgAdmin 4 versions prior to v6.19 contains a directory traversal vulnerability. A user of the product may change another user's settings or alter the database. | 6.5 | M D |
| CVE-2023-22702 | Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WPMobile.App WPMobile.App — Android and iOS Mobile Application plugin <= 11.13 versions. | 6.5 | M D |
| CVE-2022-46848 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Themeisle Visualizer: Tables and Charts Manager for WordPress plugin <= 3.9.1 versions. | 6.5 | M D |
| CVE-2023-0335 | The WP Shamsi WordPress plugin through 4.3.3 has CSRF and broken access control vulnerabilities which leads user with role as low as subscriber delete attachment. | 6.5 | M D |
| CVE-2023-0336 | The OoohBoi Steroids for Elementor WordPress plugin before 2.1.5 has CSRF and broken access control vulnerabilities which leads user with role as low as subscriber to delete attachment. | 6.5 | M D |
| CVE-2023-23728 | Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Winwar Media WP Flipclock plugin <= 1.7.4 versions. | 6.5 | M D |
| CVE-2023-25661 | TensorFlow is an Open Source Machine Learning Framework. In versions prior to 2.11.1 a malicious invalid input crashes a tensorflow model (Check Failed) and can be used to trigger a denial of service attack. A proof of concept can be constructed with the `Convolution3DTranspose` function. This Convolution3DTranspose layer is a very common API in modern neural networks. The ML models containing such vulnerable components could be deployed in ML applications or as cloud services. This failure could be potentially used to trigger a denial of service attack on ML cloud services. An attacker must have privilege to provide input to a `Convolution3DTranspose` call. This issue has been patched and users are advised to upgrade to version 2.11.1. There are no known workarounds for this vulnerability. | 6.5 | M D |
| CVE-2023-0500 | The WP Film Studio WordPress plugin before 1.3.5 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 6.5 | M D |
| CVE-2023-0501 | The WP Insurance WordPress plugin before 2.1.4 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 6.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-27927 | An authenticated malicious user could acquire the simple mail transfer protocol (SMTP) Password in cleartext format, despite it being protected and hidden behind asterisks. The attacker could then perform further attacks using the SMTP credentials. | 6.5 | M D |
| CVE-2023-0502 | The WP News WordPress plugin through 1.1.9 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 6.5 | M D |
| CVE-2023-20056 | A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. | 6.5 | M D |
| CVE-2022-48355 | The Bluetooth module has a heap out-of-bounds read vulnerability. Successful exploitation of this vulnerability can cause the Bluetooth process to crash. | 6.5 | M D |
| CVE-2022-48354 | The Bluetooth module has a heap out-of-bounds write vulnerability. Successful exploitation of this vulnerability can cause the Bluetooth process to crash. | 6.5 | M D |
| CVE-2022-24972 | This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of TP-Link TL-WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper access control. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-13911. | 6.5 | M D |
| CVE-2023-20066 | A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. | 6.5 | M D |
| CVE-2023-0816 | The Formidable Forms WordPress plugin before 6.1 uses several potentially untrusted headers to determine the IP address of the client, leading to IP Address spoofing and bypass of anti-spam protections. | 6.5 | M D |
| CVE-2023-1092 | The OAuth Single Sign On Free WordPress plugin before 6.24.2, OAuth Single Sign On Standard WordPress plugin before 28.4.9, OAuth Single Sign On Premium WordPress plugin before 38.4.9 and OAuth Single Sign On Enterprise WordPress plugin before 48.4.9 do not have CSRF checks when deleting Identity Providers (IdP), which could allow attackers to make logged in admins delete arbitrary IdP via a CSRF attack | 6.5 | M D |
| CVE-2023-1093 | The OAuth Single Sign On WordPress plugin before 6.24.2 does not have CSRF checks when discarding Identify providers (IdP), which could allow attackers to make logged in admins delete all IdP via a CSRF attack | 6.5 | M D |
| CVE-2022-46855 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WP Darko Responsive Pricing Table plugin <= 5.1.6 versions. | 6.5 | M D |
| CVE-2022-47924 | An high privileged attacker may pass crafted arguments to the validate function of csaf-validator-lib of a locally installed Secvisogram in versions < 0.1.0 wich can result in arbitrary code execution and DoS once the users triggers the validation. | 6.5 | M D |
| CVE-2023-20113 | A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. These actions could include modifying the system configuration and deleting accounts. | 6.5 | M D |
| CVE-2023-28652 | An authenticated malicious user could successfully upload a malicious image could lead to a denial-of-service condition. | 6.5 | M D |
| CVE-2023-0775 | An invalid ‘prepare write request’ command can cause the Bluetooth LE stack to run out of memory and fail to be able to handle subsequent connection requests, resulting in a denial-of-service. | 6.5 | M D |
| CVE-2022-32199 | db_convert.php in ScriptCase through 9.9.008 is vulnerable to Arbitrary File Deletion by an admin via a directory traversal sequence in the file parameter. | 6.5 | M D |
| CVE-2023-22712 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TemplatesNext TemplatesNext ToolKit plugin <= 3.2.7 versions. | 6.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-28330 | Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. | 6.5 | M D |
| CVE-2023-20861 | In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition. | 6.5 | M D |
| CVE-2023-27096 | Insecure Permissions vulnerability found in OpenGoofy Hippo4j v.1.4.3 allows attacker to obtain sensitive information via the ConfigVerifyController function of the Tenant Management module. | 6.5 | M D |
| CVE-2023-24625 | Faveo 5.0.1 allows remote attackers to obtain sensitive information via a modified user ID in an Insecure Direct Object Reference (IDOR) attack. | 6.5 | M D |
| CVE-2022-48291 | The Bluetooth module has an authentication bypass vulnerability in the pairing process. Successful exploitation of this vulnerability may affect confidentiality. | 6.5 | M D |
| CVE-2023-24834 | WisdomGarden Tronclass has improper access control when uploading file. An authenticated remote attacker with general user privilege can exploit this vulnerability to access files belonging to other users by modifying the file ID within URL. | 6.5 | M D |
| CVE-2023-23650 | Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in MainWP MainWP Code Snippets Extension plugin <= 4.0.2 versions. | 6.5 | M D |
| CVE-2023-28859 | redis-py before 4.4.4 and 4.5.x before 4.5.4 leaves a connection open after canceling an async Redis command at an inopportune time, and can send response data to the client of an unrelated request. (This could, for example, happen for a non-pipeline operation.) NOTE: the solutions for CVE-2023-28859 address data leakage across AsyncIO connections in general. | 6.5 | M D |
| CVE-2023-25721 | Veracode Scan Jenkins Plugin before 23.3.19.0, when the "Connect using proxy" option is enabled and configured with proxy credentials and when the Jenkins global system setting debug is enabled and when a scan is configured for remote agent jobs, allows users (with access to view the job log) to discover proxy credentials. | 6.5 | M D |
| CVE-2023-25667 | TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, integer overflow occurs when `2^31 <= num_frames * height * width * channels < 2^32`, for example Full HD screencast of at least 346 frames. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. | 6.5 | M D |
| CVE-2023-23864 | Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Michael Aronoff Very Simple Google Maps plugin <= 2.8.4 versions. | 6.5 | M D |
| CVE-2023-0056 | An uncontrolled resource consumption vulnerability was discovered in HAProxy which could crash the service. This issue could allow an authenticated remote attacker to run a specially crafted malicious server in an OpenShift cluster. The biggest impact is to availability. | 6.5 | M D |
| CVE-2023-28435 | Dataease is an open source data visualization and analysis tool. The permissions for the file upload interface is not checked so users who are not logged in can upload directly to the background. The file type also goes unchecked, users could upload any type of file. These vulnerabilities has been fixed in version 1.18.5. | 6.5 | M D |
| CVE-2023-24366 | An arbitrary file download vulnerability in rConfig v6.8.0 allows attackers to download sensitive files via a crafted HTTP request. | 6.5 | M D |
| CVE-2023-28640 | Apiman is a flexible and open source API Management platform. Due to a missing permissions check, an attacker with an authenticated Apiman Manager account may be able to gain access to API keys they do not have permission for if they correctly guess the URL, which includes Organisation ID, Client ID, and Client Version of the targeted non-permitted resource. While not trivial to exploit, it could be achieved by brute-forcing or guessing common names. Access to the non-permitted API Keys could allow use of other users' resources without their permission (depending on the specifics of configuration, such as whether an API key is the only form of security). Apiman 3.1.0.Final resolved this issue. Users are advised to upgrade. The only known workaround is to restrict account access. | 6.4 | M D |
| CVE-2023-21055 | In dit_hal_ioctl of dit.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244301523References: N/A | 6.4 | M D |
| CVE-2023-1566 | A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been declared as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223558 is the identifier assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1564 | A vulnerability was found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/transactions/update_status.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223556. | 6.3 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1563 | A vulnerability has been found in SourceCodester Student Study Center Desk Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/assign/assign.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223555. | 6.3 | M D |
| CVE-2023-1561 | A vulnerability, which was classified as critical, was found in code-projects Simple Online Hotel Reservation System 1.0. Affected is an unknown function of the file add_room.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. VDB-223554 is the identifier assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1675 | A vulnerability was found in SourceCodester School Registration and Fee System 1.0. It has been classified as critical. Affected is an unknown function of the file /bilal final/edit_stud.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224232. | 6.3 | M D |
| CVE-2023-1556 | A vulnerability was found in SourceCodester Judging Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file summary_results.php. The manipulation of the argument main_event_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223549 was assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1571 | A vulnerability, which was classified as critical, was found in DataGear up to 4.5.0. This affects an unknown part of the file /analysisProject/pagingQueryData. The manipulation of the argument queryOrder leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.5.1 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-223563. | 6.3 | M D |
| CVE-2023-1666 | A vulnerability has been found in SourceCodester Automatic Question Paper Generator System 1.0 and classified as critical. This vulnerability affects unknown code of the file users/classes/view_class.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224104. | 6.3 | M D |
| CVE-2015-10097 | A vulnerability was found in grinnellplans-php up to 3.0. It has been declared as critical. Affected by this vulnerability is the function interface_disp_page/interface_disp_page of the file read.php. The manipulation leads to sql injection. The attack can be launched remotely. The identifier of the patch is 57e4409e19203a94495140ff1b5a697734d17cfb. It is recommended to apply a patch to fix this issue. The identifier VDB-223801 was assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-25594 | A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. | 6.3 | M D |
| CVE-2023-1558 | A vulnerability classified as critical has been found in Simple and Beautiful Shopping Cart System 1.0. This affects an unknown part of the file uploadera.php. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223551. | 6.3 | M D |
| CVE-2023-1557 | A vulnerability was found in SourceCodester E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ecommerce/admin/user/controller.php?action=edit of the component Username Handler. The manipulation of the argument USERID leads to improper access controls. The attack may be launched remotely. VDB-223550 is the identifier assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1634 | A vulnerability was found in OTCMS 6.72. It has been classified as critical. Affected is the function UseCurl of the file /admin/info_deal.php of the component URL Parameter Handler. The manipulation leads to server-side request forgery. 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-224016. | 6.3 | M D |
| CVE-2023-25197 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation apache fineract. Authorized users may be able to exploit this for limited impact on components. This issue affects apache fineract: from 1.4 through 1.8.2. | 6.3 | M D |
| CVE-2023-1606 | A vulnerability was found in novel-plus 3.6.2 and classified as critical. Affected by this issue is some unknown functionality of the file DictController.java. The manipulation of the argument orderby leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223736. | 6.3 | M D |
| CVE-2023-1608 | A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been declared as critical. This vulnerability affects the function getAdminList of the file /api/admin/store/product/list. The manipulation of the argument cateId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223738 is the identifier assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1610 | A vulnerability, which was classified as critical, has been found in Rebuild up to 3.2.3. Affected by this issue is some unknown functionality of the file /project/tasks/list. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-223742 is the identifier assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1612 | A vulnerability, which was classified as critical, was found in Rebuild up to 3.2.3. This affects an unknown part of the file /files/list-file. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-223743. | 6.3 | M D |
| CVE-2023-1589 | A vulnerability has been found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This vulnerability affects the function exec of the file admin/operations/approve_delete.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223654 is the identifier assigned to this vulnerability. | 6.3 | M D |
| CVE-2023-1590 | A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This issue affects the function exec of the file admin/operations/currency.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223655. | 6.3 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1591 | A vulnerability classified as critical has been found in SourceCodester Automatic Question Paper Generator System 1.0. This affects an unknown part of the file classes/Users.php?f=save_ruser. The manipulation of the argument id/email leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-223659. | 6.3 | M D |
| CVE-2023-1592 | A vulnerability classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. This vulnerability affects unknown code of the file admin/courses/view_class.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-223660. | 6.3 | M D |
| CVE-2023-28438 | Pimcore is an open source data and experience management platform. Prior to version 10.5.19, since a user with 'report' permission can already write arbitrary SQL queries and given the fact that this endpoint is using the GET method (no CSRF protection), an attacker can inject an arbitrary query by manipulating a user to click on a link. Users should upgrade to version 10.5.19 to receive a patch or, as a workaround, may apply the patch manually. | 6.2 | M D |
| CVE-2023-1410 | Grafana is an open-source platform for monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description. Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix. | 6.2 | M D |
| CVE-2023-26913 | EVOLUCARE ECSIMAGING (aka ECS Imaging) < 6.21.5 is vulnerable to Cross Site Scripting (XSS) via new_movie. php. | 6.1 | M D |
| CVE-2022-45004 | Gophish through 0.12.1 was discovered to contain a cross-site scripting (XSS) vulnerability via a crafted landing page. | 6.1 | M D |
| CVE-2023-28884 | In MISP 2.4.169, app/Lib/Tools/CustomPaginationTool.php allows XSS in the community index. | 6.1 | M D |
| CVE-2023-24839 | HGiga MailSherlock's specific function has insufficient filtering for user input. An unauthenticated remote attacker can exploit this vulnerability to inject JavaScript, conducting a reflected XSS attack. | 6.1 | M D |
| CVE-2023-27054 | A cross-site scripting (XSS) vulnerability in MiroTalk P2P before commit f535b35 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter under the settings module. | 6.1 | M D |
| CVE-2023-20082 | A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. | 6.1 | M D |
| CVE-2023-1051 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in As Koc Energy Web Report System allows Reflected XSS.This issue affects Web Report System: before 23.03.10. | 6.1 | M D |
| CVE-2023-27245 | A cross-site scripting (XSS) vulnerability in File Management Project 1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field under the Edit User module. | 6.1 | M D |
| CVE-2023-22300 | An unauthenticated remote attacker could force all authenticated users, such as administrative users, to perform unauthorized actions by viewing the logs. This action would also grant the attacker privilege escalation. | 6.1 | M D |
| CVE-2020-24857 | Cross Site Scripting vulnerabilty found in IXPManager v.5.6.0 allows attackers to excute arbitrary code via the looking glass component. | 6.1 | M D |
| CVE-2023-28650 | An unauthenticated remote attacker could provide a malicious link and trick an unsuspecting user into clicking on it. If clicked, the attacker could execute the malicious JavaScript (JS) payload in the target's security context. | 6.1 | M D |
| CVE-2023-28332 | If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. | 6.1 | M D |
| CVE-2023-28331 | Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. | 6.1 | M D |
| CVE-2023-27008 | A Cross-site scripting (XSS) vulnerability in the function encrypt_password() in login.tmpl.php in ATutor 2.2.1 allows remote attackers to inject arbitrary web script or HTML via the token parameter. | 6.1 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-27241 | SourceCodester Water Billing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the lastname text box under the Add Client module. | 6.1 | M D |
| CVE-2022-2237 | A flaw was found in the Keycloak Node.js Adapter. This flaw allows an attacker to benefit from an Open Redirect vulnerability in the checkSso function. | 6.1 | M D |
| CVE-2023-1544 | A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. This flaw allows a crafted guest driver to allocate and initialize a huge number of page tables to be used as a ring of descriptors for CQ and async events, potentially leading to an out-of-bounds read and crash of QEMU. | 6.0 | M D |
| CVE-2023-22716 | Auth. (admin+) Cross-Site Scripting vulnerability in OOPSpam OOPSpam Anti-Spam plugin <= 1.1.35 versions. | 5.9 | M D |
| CVE-2023-26008 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ajay D'Souza Top 10 – Popular posts plugin for WordPress plugin <= 3.2.4 versions. | 5.9 | M D |
| CVE-2022-47589 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in this.Functional CTT Expresso para WooCommerce plugin <= 3.2.11 versions. | 5.9 | M D |
| CVE-2023-22707 | Auth. (author+) Cross-Site Scripting (XSS) vulnerability in Wpsoul Greenshift – animation and page builder blocks plugin <= 4.9.9 versions. | 5.9 | M D |
| CVE-2023-25992 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CreativeMindsSolutions CM Answers plugin <= 3.1.9 versions. | 5.9 | M D |
| CVE-2023-25704 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mehjabin Orthi Interactive SVG Image Map Builder plugin <= 1.0 versions. | 5.9 | M D |
| CVE-2022-47170 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin <= 1.5.48 versions. | 5.9 | M D |
| CVE-2022-46863 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Event Manager plugin <= 9.6.4 versions. | 5.9 | M D |
| CVE-2023-25456 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Klaviyo, Inc. Klaviyo plugin <= 3.0.7 versions. | 5.9 | M D |
| CVE-2023-23707 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Unrestricted Upload of File with Dangerous Type vulnerability in Awsm Innovations Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files allows Stored XSS via upload of SVG and HTML files. This issue affects Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files plugin <= 2.7.1 versions. | 5.9 | M D |
| CVE-2023-22715 | Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Lester 'GaMerZ' Chan WP-CommentNavi plugin <= 1.12.1 versions. | 5.9 | M D |
| CVE-2022-47173 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in nasirahmed Connect Contact Form 7, WooCommerce To Google Sheets & Other Platforms – Advanced Form Integration plugin <= 1.62.0 versions. | 5.9 | M D |
| CVE-2023-28422 | Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin for WooCommerce <= 3.8.6. versions. | 5.9 | M D |
| CVE-2023-23722 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media WP eBay Product Feeds plugin <= 3.3.1 versions. | 5.9 | M D |
| CVE-2023-1436 | An infinite recursion is triggered in Jettison when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. This leads to a StackOverflowError exception being thrown. | 5.9 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-28436 | Tailscale is software for using Wireguard and multi-factor authentication (MFA). A vulnerability identified in the implementation of Tailscale SSH starting in version 1.34.0 and prior to prior to 1.38.2 in FreeBSD allows commands to be run with a higher privilege group ID than that specified in Tailscale SSH access rules. A difference in the behavior of the FreeBSD `setgroups` system call from POSIX meant that the Tailscale client running on a FreeBSD-based operating system did not appropriately restrict groups on the host when using Tailscale SSH. When accessing a FreeBSD host over Tailscale SSH, the egid of the tailscaled process was used instead of that of the user specified in Tailscale SSH access rules. Tailscale SSH commands may have been run with a higher privilege group ID than that specified in Tailscale SSH access rules if they met all of the following criteria: the destination node was a FreeBSD device with Tailscale SSH enabled; Tailscale SSH access rules permitted access for non-root users; and a non-interactive SSH session was used. Affected users should upgrade to version 1.38.2 to remediate the issue. | 5.7 | M D |
| CVE-2021-3844 | Rapid7 InsightVM suffers from insufficient session expiration when an administrator performs a security relevant edit on an existing, logged on user. For example, if a user's password is changed by an administrator due to an otherwise unrelated credential leak, that user account's current session is still valid after the password change, potentially allowing the attacker who originally compromised the credential to remain logged in and able to cause further damage. This vulnerability is mitigated by the use of the Platform Login feature. This issue is related to CVE-2019-5638. | 5.7 | M D |
| CVE-2023-28448 | Versionize is a framework for version tolerant serializion/deserialization of Rust data structures, designed for usecases that need fast deserialization times and minimal size overhead. An issue was discovered in the ‘Versionize::deserialize’ implementation provided by the ‘versionize’ crate for ‘vmm_sys_utils::fam::FamStructWrapper', which can lead to out of bounds memory accesses. The impact started with version 0.1.1. The issue was corrected in version 0.1.10 by inserting a check that verifies, for any deserialized header, the lengths of compared flexible arrays are equal and aborting deserialization otherwise. | 5.7 | M D |
| CVE-2023-20929 | In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700 | 5.5 | M D |
| CVE-2023-26344 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26345 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26343 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26342 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26346 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26348 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26352 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26353 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26349 | Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26350 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26351 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26340 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-26354 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20952 | In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 | 5.5 | M D |
| CVE-2023-26355 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-20962 | In getSliceEndItem of MediaVolumePreferenceController.java, there is a possible way to start foreground activity from the background due to an unsafe PendingIntent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256590210 | 5.5 | M D |
| CVE-2023-20972 | In btm_vendor_specific_evt of btm_devctl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304665 | 5.5 | M D |
| CVE-2023-20973 | In btm_create_conn_cancel_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568245 | 5.5 | M D |
| CVE-2023-20974 | In btm_ble_add_resolving_list_entry_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260078907 | 5.5 | M D |
| CVE-2023-20979 | In GetNextSourceDataPacket of bta_av_co.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259939364 | 5.5 | M D |
| CVE-2023-20980 | In btu_ble_ll_conn_param_upd_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260230274 | 5.5 | M D |
| CVE-2023-26341 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2022-20467 | In isBluetoothShareUri of BluetoothOppUtility.java, there is a possible incorrect file read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225880741 | 5.5 | M D |
| CVE-2023-26339 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-1677 | A vulnerability was found in DriverGenius 9.70.0.346. It has been rated as problematic. Affected by this issue is the function 0x9c40a0c8/0x9c40a0dc/0x9c40a0e0/0x9c40a0d8/0x9c4060d4/0x9c402004/0x9c402088/0x9c40208c/0x9c4060d0/0x9c4060cc/0x9c4060c4/0x9c402084 in the library mydrivers64.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-224234 is the identifier assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-1289 | A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. | 5.5 | M D |
| CVE-2023-25878 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-25877 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-25876 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-25875 | Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-1637 | A flaw that boot CPU could be vulnerable for the speculative execution behavior kind of attacks in the Linux kernel X86 CPU Power management options functionality was found in the way user resuming CPU from suspend-to-RAM. A local user could use this flaw to potentially get unauthorized access to some memory of the CPU similar to the speculative execution behavior kind of attacks. | 5.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-26924 | LLVM a0dab4950 has a segmentation fault in mlir::outlineSingleBlockRegion. NOTE: third parties dispute this because the LLVM security policy excludes "Language front-ends ... for which a malicious input file can cause undesirable behavior." | 5.5 | M D |
| CVE-2023-21033 | In addNetwork of WifiManager.java, there is a possible way to trigger a persistent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244713323 | 5.5 | M D |
| CVE-2022-3101 | A flaw was found in tripleo-ansible. Due to an insecure default configuration, the permissions of a sensitive file are not sufficiently restricted. This flaw allows a local attacker to use brute force to explore the relevant directory and discover the file, leading to information disclosure of important configuration details from the OpenStack deployment. | 5.5 | M D |
| CVE-2022-3146 | A flaw was found in tripleo-ansible. Due to an insecure default configuration, the permissions of a sensitive file are not sufficiently restricted. This flaw allows a local attacker to use brute force to explore the relevant directory and discover the file. This issue leads to information disclosure of important configuration details from the OpenStack deployment. | 5.5 | M D |
| CVE-2023-25263 | In Stimulsoft Designer (Desktop) 2023.1.5, and 2023.1.4, once an attacker decompiles the Stimulsoft.report.dll the attacker is able to decrypt any connectionstring stored in .mrt files since a static secret is used. The secret does not differ between the tested versions and different operating systems. | 5.5 | M D |
| CVE-2023-1249 | A use-after-free flaw was found in the Linux kernel's core dump subsystem. This flaw allows a local user to crash the system. Only if patch 390031c94211 ("coredump: Use the vma snapshot in fill_files_note") not applied yet, then kernel could be affected. | 5.5 | M D |
| CVE-2023-21029 | In register of UidObserverController.java, there is a missing permission check. This could lead to local information disclosure of app usage with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-217934898 | 5.5 | M D |
| CVE-2023-26338 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-20859 | In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. | 5.5 | M D |
| CVE-2023-1076 | A flaw was found in the Linux Kernel. The tun/tap sockets have their socket UID hardcoded to 0 due to a type confusion in their initialization function. While it will be often correct, as tuntap devices require CAP_NET_ADMIN, it may not always be the case, e.g., a non-root user only having that capability. This would make tun/tap sockets being incorrectly treated in filtering/routing decisions, possibly bypassing network filters. | 5.5 | M D |
| CVE-2023-1074 | A memory leak flaw was found in the Linux kernel's Stream Control Transmission Protocol. This issue may occur when a user starts a malicious networking service and someone connects to this service. This could allow a local user to starve resources, causing a denial of service. | 5.5 | M D |
| CVE-2023-21036 | In BitmapExport.java, there is a possible failure to truncate images due to a logic error in the code.Product: AndroidVersions: Android kernelAndroid ID: A-264261868References: N/A | 5.5 | M D |
| CVE-2023-21026 | In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254681548 | 5.5 | M D |
| CVE-2023-25722 | A credential-leak issue was discovered in related Veracode products before 2023-03-27. Veracode Scan Jenkins Plugin before 23.3.19.0, when configured for remote agent jobs, invokes the Veracode Java API Wrapper in a manner that allows local users (with OS-level access of the Jenkins remote) to discover Veracode API credentials by listing the process and its arguments. Veracode Scan Jenkins Plugin before 23.3.19.0, when configured for remote agent jobs and when the "Connect using proxy" option is enabled and configured with proxy credentials, allows local users of the Jenkins remote to discover proxy credentials by listing the process and its arguments. Veracode Azure DevOps Extension before 3.20.0 invokes the Veracode Java API Wrapper in a manner that allows local users (with OS-level access to the Azure DevOps Services cloud infrastructure or Azure DevOps Server) to discover Veracode API credentials by listing the process and its arguments. Veracode Azure DevOps Extension before 3.20.0, when configured with proxy credentials, allows users (with shell access to the Azure DevOps Services cloud infrastructure or Azure DevOps Server) to discover proxy credentials by listing the process and its arguments. | 5.5 | M D |
| CVE-2020-36691 | An issue was discovered in the Linux kernel before 5.8. lib/nlattr.c allows attackers to cause a denial of service (unbounded recursion) via a nested Netlink policy with a back reference. | 5.5 | M D |
| CVE-2021-3684 | A vulnerability was found in OpenShift Assisted Installer. During generation of the Discovery ISO, image pull secrets were leaked as plaintext in the installation logs. An authenticated user could exploit this by re-using the image pull secret to pull container images from the registry as the associated user. | 5.5 | M D |
| CVE-2023-1644 | A vulnerability was found in IObit Malware Fighter 9.4.0.776 and classified as problematic. Affected by this issue is the function 0x8018E010 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224024. | 5.5 | M D |
| CVE-2022-20499 | In validateForCommonR1andR2 of PasspointConfiguration.java, uncaught errors in parsing stored configs could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-246539931 | 5.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-42528 | In ffa_mrd_prot of shared_mem.c, there is a possible ID due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242203672References: N/A | 5.5 | M D |
| CVE-2023-20910 | In add of WifiNetworkSuggestionsManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. | 5.5 | M D |
| CVE-2023-1645 | A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been classified as problematic. This affects the function 0x8018E008 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-224025 was assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-26356 | Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-1643 | A vulnerability has been found in IObit Malware Fighter 9.4.0.776 and classified as problematic. Affected by this vulnerability is the function 0x8001E000/0x8001E004/0x8001E018/0x8001E01C/0x8001E024/0x8001E040 in the library ImfHpRegFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224023. | 5.5 | M D |
| CVE-2023-27754 | vox2mesh 1.0 has stack-overflow in main.cpp, this is stack-overflow caused by incorrect use of memcpy() funciton. The flow allows an attacker to cause a denial of service (abort) via a crafted file. | 5.5 | M D |
| CVE-2023-1628 | A vulnerability classified as problematic has been found in Jianming Antivirus 16.2.2022.418. Affected is an unknown function in the library kvcore.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-224010 is the identifier assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-1630 | A vulnerability, which was classified as problematic, has been found in JiangMin Antivirus 16.2.2022.418. Affected by this issue is the function 0x222000 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224012. | 5.5 | M D |
| CVE-2023-1631 | A vulnerability, which was classified as problematic, was found in JiangMin Antivirus 16.2.2022.418. This affects the function 0x222010 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-224013 was assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-25595 | A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. | 5.5 | M D |
| CVE-2023-1583 | A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALLOC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. | 5.5 | M D |
| CVE-2023-25862 | Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | M D |
| CVE-2023-20996 | In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749764 | 5.5 | M D |
| CVE-2023-20997 | In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749702 | 5.5 | M D |
| CVE-2023-20998 | In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936 | 5.5 | M D |
| CVE-2023-20999 | In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467 | 5.5 | M D |
| CVE-2023-27249 | swfdump v0.9.2 was discovered to contain a heap buffer overflow in the function swf_GetPlaceObject at swfobject.c. | 5.5 | M D |
| CVE-2023-1638 | A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been rated as problematic. Affected by this issue is the function 0x8001E024/0x8001E040 in the library ImfRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-224018 is the identifier assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-21019 | In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242379731 | 5.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1627 | A vulnerability was found in Jianming Antivirus 16.2.2022.418. It has been rated as problematic. This issue affects some unknown processing in the library kvcore.sys of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier VDB-224009 was assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-1639 | A vulnerability classified as problematic has been found in IObit Malware Fighter 9.4.0.776. This affects the function 0x8001E04C in the library ImfRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224019. | 5.5 | M D |
| CVE-2023-1642 | A vulnerability, which was classified as problematic, was found in IObit Malware Fighter 9.4.0.776. Affected is the function 0x222034/0x222038/0x22203C/0x222040 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-224022 is the identifier assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-1640 | A vulnerability classified as problematic was found in IObit Malware Fighter 9.4.0.776. This vulnerability affects the function 0x222010 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224020. | 5.5 | M D |
| CVE-2023-21016 | In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884 | 5.5 | M D |
| CVE-2023-1641 | A vulnerability, which was classified as problematic, has been found in IObit Malware Fighter 9.4.0.776. This issue affects the function 0x222018 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-224021 was assigned to this vulnerability. | 5.5 | M D |
| CVE-2023-22258 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22263 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22266 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22265 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-28655 | A malicious user could leverage this vulnerability to escalate privileges or perform unauthorized actions in the context of the targeted privileged users. | 5.4 | M D |
| CVE-2023-28666 | The InPost Gallery WordPress plugin, in versions < 2.2.2, is affected by a reflected cross-site scripting vulnerability in the 'imgurl' parameter to the add_inpost_gallery_slide_item action, which can only be triggered by an authenticated user. | 5.4 | M D |
| CVE-2023-22264 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-0272 | The NEX-Forms WordPress plugin before 8.3.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | M D |
| CVE-2023-22252 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. | 5.4 | M D |
| CVE-2023-0823 | The Cookie Notice & Compliance for GDPR / CCPA WordPress plugin before 2.4.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | M D |
| CVE-2023-0491 | The Schedulicity WordPress plugin through 2.21 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. | 5.4 | M D |
| CVE-2023-22253 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. | 5.4 | M D |
| CVE-2023-22262 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-22261 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-0395 | The menu shortcode WordPress plugin through 1.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. | 5.4 | M D |
| CVE-2023-22260 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22259 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22256 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22257 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. | 5.4 | M D |
| CVE-2023-22254 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. | 5.4 | M D |
| CVE-2023-0660 | The Smart Slider 3 WordPress plugin before 3.5.1.14 does not properly validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | M D |
| CVE-2023-25018 | RIFARTEK IOT Wall transportation function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can inject JavaScript to perform reflected XSS (Reflected Cross-site scripting) attack. | 5.4 | M D |
| CVE-2022-45843 | Auth. (contributor+) Stored Cross-Site Scripting vulnerability in Nextend Smart Slider 3 plugin <= 3.5.1.9 versions. | 5.4 | M D |
| CVE-2023-22269 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. | 5.4 | M D |
| CVE-2023-0589 | The WP Image Carousel WordPress plugin through 1.0.2 does not sanitise and escape some parameters, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks. | 5.4 | M D |
| CVE-2023-21615 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. | 5.4 | M D |
| CVE-2023-28664 | The Meta Data and Taxonomies Filter WordPress plugin, in versions < 1.3.1, is affected by a reflected cross-site scripting vulnerability in the 'tax_name' parameter of the mdf_get_tax_options_in_widget action, which can only be triggered by an authenticated user. | 5.4 | M D |
| CVE-2023-28665 | The Woo Bulk Price Update WordPress plugin, in versions < 2.2.2, is affected by a reflected cross-site scripting vulnerability in the 'page' parameter to the techno_get_products action, which can only be triggered by an authenticated user. | 5.4 | M D |
| CVE-2023-27242 | SourceCodester Loan Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Type parameter under the Edit Loan Types module. | 5.4 | M D |
| CVE-2022-30705 | Cross-Site Request Forgery (CSRF) vulnerability in Pankaj Jha WordPress Ping Optimizer plugin <= 2.35.1.2.3 versions. | 5.4 | M D |
| CVE-2023-25924 | IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. | 5.4 | M D |
| CVE-2023-22902 | Openfind Mail2000 file uploading function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject JavaScript, conducting an XSS attack. | 5.4 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1069 | The Complianz WordPress plugin before 6.4.2, Complianz Premium WordPress plugin before 6.4.2 do not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | M D |
| CVE-2023-28629 | GoCD is an open source continuous delivery server. GoCD versions before 23.1.0 are vulnerable to a stored XSS vulnerability, where pipeline configuration with a malicious pipeline label configuration can affect browser display of pipeline runs generated from that configuration. An attacker that has permissions to configure GoCD pipelines could include JavaScript elements within the label template, causing a XSS vulnerability to be triggered for any users viewing the Value Stream Map or Job Details for runs of the affected pipeline, potentially allowing them to perform arbitrary actions within the victim's browser context rather than their own. This issue has been fixed in GoCD 23.1.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. | 5.4 | M D |
| CVE-2023-21616 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. | 5.4 | M D |
| CVE-2023-28628 | lambdaisland/uri is a pure Clojure/ClojureScript URI library. In versions prior to 1.14.120 `authority-regex` allows an attacker to send malicious URLs to be parsed by the `lambdaisland/uri` and return the wrong authority. This issue is similar to but distinct from CVE-2020-8910. The regex in question doesn't handle the backslash (`\`) character in the username correctly, leading to a wrong output. ex. a payload of `https://example.com\\@google.com` would return that the host is `google.com`, but the correct host should be `example.com`. Given that the library returns the wrong authority this may be abused to bypass host restrictions depending on how the library is used in an application. Users are advised to upgrade. There are no known workarounds for this vulnerability. | 5.4 | M D |
| CVE-2023-1646 | A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been declared as critical. This vulnerability affects the function 0x8018E000/0x8018E004 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to stack-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. VDB-224026 is the identifier assigned to this vulnerability. | 5.3 | M D |
| CVE-2023-28631 | comrak is a CommonMark + GFM compatible Markdown parser and renderer written in rust. A Comrak AST can be constructed manually by a program instead of parsing a Markdown document with `parse_document`. This AST can then be converted to HTML via `html::format_document_with_plugins`. However, the HTML formatting code assumes that the AST is well-formed. For example, many AST notes contain `[u8]` fields which the formatting code assumes is valid UTF-8 data. Several bugs can be triggered if this is not the case. Version 0.17.0 contains adjustments to the AST, storing strings instead of unvalidated byte arrays. Users are advised to upgrade. Users unable to upgrade may manually validate UTF-8 correctness of all data when assigning to `&[u8]` and `Vec<u8>` fields in the AST. This issue is also tracked as `GHSL-2023-049`. | 5.3 | M D |
| CVE-2023-28818 | An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be downloaded and installed on collectors. | 5.3 | M D |
| CVE-2023-25818 | Nextcloud server is an open source, personal cloud implementation. In affected versions a malicious user could try to reset the password of another user and then brute force the 62^21 combinations for the password reset token. As of commit `704eb3aa` password reset attempts are now throttled. Note that 62^21 combinations would significant compute resources to brute force. None the less it is recommended that the Nextcloud Server is upgraded to 24.0.10 or 25.0.4. There are no known workarounds for this vulnerability. | 5.3 | M D |
| CVE-2022-37940 | Potential security vulnerabilities have been identified in the HPE FlexFabric 5700 Switch Series. These vulnerabilities could be remotely exploited to allow host header injection and URL redirection. HPE has made the following software to resolve the vulnerability in HPE FlexFabric 5700 Switch Series version R2432P61 or later. | 5.3 | M D |
| CVE-2023-28152 | An issue was discovered in Independentsoft JWord before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. | 5.3 | M D |
| CVE-2023-22271 | Experience Manager versions 6.5.15.0 (and earlier) are affected by a Weak Cryptography for Passwords vulnerability that can lead to a security feature bypass. A low-privileged attacker can exploit this in order to decrypt a user's password. The attack complexity is high since a successful exploitation requires to already have in possession this encrypted secret. | 5.3 | M D |
| CVE-2023-1626 | A vulnerability was found in Jianming Antivirus 16.2.2022.418. It has been declared as critical. This vulnerability affects unknown code in the library kvcore.sys of the component IoControlCode Handler. The manipulation leads to memory corruption. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224008. | 5.3 | M D |
| CVE-2023-28470 | In Couchbase Server 5 through 7 before 7.1.4, the nsstats endpoint is accessible without authentication. | 5.3 | M D |
| CVE-2023-22250 | Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the availability of a user's minor feature. Exploitation of this issue does not require user interaction. | 5.3 | M D |
| CVE-2023-28866 | In the Linux kernel through 6.2.8, net/bluetooth/hci_sync.c allows out-of-bounds access because amp_init1[] and amp_init2[] are supposed to have an intentionally invalid element, but do not. | 5.3 | M D |
| CVE-2023-24842 | HGiga MailSherlock has vulnerability of insufficient access control. An unauthenticated remote user can exploit this vulnerability to access partial content of another user’s mail by changing user ID and mail ID within URL. | 5.3 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1679 | A vulnerability classified as critical was found in DriverGenius 9.70.0.346. This vulnerability affects the function 0x9C406104/0x9C40A108 in the library mydrivers64.sys of the component IOCTL Handler. The manipulation leads to memory corruption. 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-224236. | 5.3 | M D |
| CVE-2022-48361 | The Always On Display (AOD) has a path traversal vulnerability in theme files. Successful exploitation of this vulnerability may cause a failure in reading AOD theme resources. | 5.3 | M D |
| CVE-2023-28150 | An issue was discovered in Independentsoft JODF before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. | 5.3 | M D |
| CVE-2023-0465 | Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. | 5.3 | M D |
| CVE-2023-0466 | The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification. As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument. Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications. | 5.3 | M D |
| CVE-2023-1678 | A vulnerability classified as critical has been found in DriverGenius 9.70.0.346. This affects the function 0x9C40A0D8/0x9C40A0DC/0x9C40A0E0 in the library mydrivers64.sys of the component IOCTL Handler. The manipulation leads to memory corruption. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224235. | 5.3 | M D |
| CVE-2023-28151 | An issue was discovered in Independentsoft JSpreadsheet before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. | 5.3 | M D |
| CVE-2023-1629 | A vulnerability classified as critical was found in JiangMin Antivirus 16.2.2022.418. Affected by this vulnerability is the function 0x222010 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224011. | 5.3 | M D |
| CVE-2023-28626 | comrak is a CommonMark + GFM compatible Markdown parser and renderer written in rust. A range of quadratic parsing issues are present in Comrak. These can be used to craft denial-of-service attacks on services that use Comrak to parse Markdown. This issue has been addressed in version 0.17.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as `GHSL-2023-047` | 5.3 | M D |
| CVE-2023-0326 | An issue has been discovered in GitLab DAST API scanner affecting all versions starting from 1.6.50 before 2.11.0, where Authorization headers was leaked in vulnerability report evidence. | 5.0 | M D |
| CVE-2023-26361 | Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in Arbitrary file system read. Exploitation of this issue does not require user interaction, but does require administrator privileges. | 4.9 | M D |
| CVE-2023-22249 | Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and earlier) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. | 4.8 | M D |
| CVE-2022-3686 | A vulnerability exists in a SDM600 endpoint. An attacker could exploit this vulnerability by running multiple parallel requests, the SDM600 web services become busy rendering the application unresponsive. This issue affects: All SDM600 versions prior to version 1.2 FP3 HF4 (Build Nr. 1.2.23000.291) List of CPEs: * cpe:2.3:a:hitachienergy:sdm600:1.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.1:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.9002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.10002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.11002.149:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.12002.222:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.13002.72:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.44:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.92:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.108:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.182:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.257:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.342:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.447:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.481:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.506:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.14002.566:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.20000.3174:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.291:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.931:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.21000.105:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:sdm600:1.2.23000.291:*:*:*:*:*:*:* | 4.8 | M D |
| CVE-2023-28114 | `cilium-cli` is the command line interface to install, manage, and troubleshoot Kubernetes clusters running Cilium. Prior to version 0.13.2,`cilium-cli`, when used to configure cluster mesh functionality, can remove the enforcement of user permissions on the `etcd` store used to mirror local cluster information to remote clusters. Users who have set up cluster meshes using the Cilium Helm chart are not affected by this issue. Due to an incorrect mount point specification, the settings specified by the `initContainer` that configures `etcd` users and their permissions are overwritten when using `cilium-cli` to configure a cluster mesh. An attacker who has already gained access to a valid key and certificate for an `etcd` cluster compromised in this manner could then modify state in that `etcd` cluster. This issue is patched in `cilium-cli` 0.13.2. As a workaround, one may use Cilium's Helm charts to create their cluster. | 4.8 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1025 | The Simple File List WordPress plugin before 6.0.10 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). | 4.8 | M D |
| CVE-2023-1400 | The Modern Events Calendar Lite WordPress plugin before 6.5.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). | 4.8 | M D |
| CVE-2022-44742 | Auth. (admin+) Stored Cross-Site Scripting vulnerability in Yannick Lefebvre Community Events plugin <= 1.4.8 versions. | 4.8 | M D |
| CVE-2023-26958 | Phpgurukul Park Ticketing Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Admin Name parameter. | 4.8 | M D |
| CVE-2023-1595 | A vulnerability has been found in novel-plus 3.6.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file common/log/list. The manipulation of the argument sort leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223663. | 4.7 | M D |
| CVE-2023-1559 | A vulnerability classified as problematic was found in SourceCodester Storage Unit Rental Management System 1.0. This vulnerability affects unknown code of the file classes/Users.php?f=save. The manipulation leads to unrestricted upload. 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-223552. | 4.7 | M D |
| CVE-2023-1607 | A vulnerability was found in novel-plus 3.6.2. It has been classified as critical. This affects an unknown part of the file /common/sysFile/list. The manipulation of the argument sort leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223737 was assigned to this vulnerability. | 4.7 | M D |
| CVE-2023-28439 | CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability has been discovered affecting Iframe Dialog and Media Embed packages. The vulnerability may trigger a JavaScript code after fulfilling special conditions: using one of the affected packages on a web page with missing proper Content Security Policy configuration; initializing the editor on an element and using an element other than `<textarea>` as a base; and destroying the editor instance. This vulnerability might affect a small percentage of integrators that depend on dynamic editor initialization/destroy mechanism. A fix is available in CKEditor4 version 4.21.0. In some rare cases, a security fix may be considered a breaking change. Starting from version 4.21.0, the Iframe Dialog plugin applies the `sandbox` attribute by default, which restricts JavaScript code execution in the iframe element. To change this behavior, configure the `config.iframe_attributes` option. Also starting from version 4.21.0, the Media Embed plugin regenerates the entire content of the embed widget by default. To change this behavior, configure the `config.embed_keepOriginalContent` option. Those who choose to enable either of the more permissive options or who cannot upgrade to a patched version should properly configure Content Security Policy to avoid any potential security issues that may arise from embedding iframe elements on their web page. | 4.7 | M D |
| CVE-2023-21031 | In setPowerMode of HWC2.cpp, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242688355 | 4.7 | M D |
| CVE-2023-0590 | A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected. | 4.7 | M D |
| CVE-2022-48428 | In JetBrains TeamCity before 2022.10.3 stored XSS on the SSH keys page was possible | 4.6 | M D |
| CVE-2022-48427 | In JetBrains TeamCity before 2022.10.3 stored XSS on “Pending changes” and “Changes” tabs was possible | 4.6 | M D |
| CVE-2023-20097 | A vulnerability in Cisco access points (AP) software could allow an authenticated, local attacker to inject arbitrary commands and execute them with root privileges. This vulnerability is due to improper input validation of commands that are issued from a wireless controller to an AP. An attacker with Administrator access to the CLI of the controller could exploit this vulnerability by issuing a command with crafted arguments. A successful exploit could allow the attacker to gain full root access on the AP. | 4.6 | M D |
| CVE-2022-48429 | In JetBrains Hub before 2022.3.15573, 2022.2.15572, 2022.1.15583 reflected XSS in dashboards was possible | 4.6 | M D |
| CVE-2022-48426 | In JetBrains TeamCity before 2022.10.3 stored XSS in Perforce connection settings was possible | 4.6 | M D |
| CVE-2023-20987 | In btm_read_link_quality_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure over Bluetooth with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569414 | 4.5 | M D |
| CVE-2023-20992 | In on_iso_link_quality_read of btm_iso_impl.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568750 | 4.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20988 | In btm_read_rssi_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569232 | 4.5 | M D |
| CVE-2023-25596 | A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager. | 4.5 | M D |
| CVE-2023-21008 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030100 | 4.4 | M D |
| CVE-2023-21010 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029915 | 4.4 | M D |
| CVE-2023-21007 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029965 | 4.4 | M D |
| CVE-2023-21006 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030027 | 4.4 | M D |
| CVE-2023-21009 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029925 | 4.4 | M D |
| CVE-2023-20968 | In multiple functions of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235935 | 4.4 | M D |
| CVE-2023-21025 | In ufdt_local_fixup_prop of ufdt_overlay.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254929746 | 4.4 | M D |
| CVE-2023-21011 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029912 | 4.4 | M D |
| CVE-2023-20981 | In btu_ble_rc_param_req_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256165737 | 4.4 | M D |
| CVE-2023-20969 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236313 | 4.4 | M D |
| CVE-2023-20970 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236005 | 4.4 | M D |
| CVE-2023-21032 | In _ufdt_output_node_to_fdt of ufdt_convert.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-248085351 | 4.4 | M D |
| CVE-2023-21046 | In ConvertToHalMetadata of aidl_utils.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253424924References: N/A | 4.4 | M D |
| CVE-2023-20977 | In btm_ble_read_remote_features_complete of btm_ble_gap.cc, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure if the firmware were compromised with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254445952 | 4.4 | M D |
| CVE-2023-21012 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029812 | 4.4 | M D |
| CVE-2023-21047 | In ConvertToHalMetadata of aidl_utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-256166866References: N/A | 4.4 | M D |
| CVE-2023-21045 | When cpif handles probe failures, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323725References: N/A | 4.4 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20956 | In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240140929 | 4.4 | M D |
| CVE-2023-20986 | In btm_ble_clear_resolving_list_completecomplete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304475 | 4.4 | M D |
| CVE-2023-21049 | In append_camera_metadata of camera_metadata.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-236688120References: N/A | 4.4 | M D |
| CVE-2023-21039 | In dumpstateBoard of Dumpstate.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783650References: N/A | 4.4 | M D |
| CVE-2023-21044 | In init of VendorGraphicBufferMeta, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253425086References: N/A | 4.4 | M D |
| CVE-2023-27247 | Cynet Client Agent v4.6.0.8010 allows attackers with Administrator rights to disable the EDR functions by disabling process privilege tokens. | 4.4 | M D |
| CVE-2023-20989 | In btm_ble_write_adv_enable_complete of btm_ble_gap.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568367 | 4.4 | M D |
| CVE-2023-20029 | A vulnerability in the Meraki onboarding feature of Cisco IOS XE Software could allow an authenticated, local attacker to gain root level privileges on an affected device. This vulnerability is due to insufficient memory protection in the Meraki onboarding feature of an affected device. An attacker could exploit this vulnerability by modifying the Meraki registration parameters. A successful exploit could allow the attacker to elevate privileges to root. | 4.4 | M D |
| CVE-2023-20990 | In btm_ble_rand_enc_complete of btm_ble.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568354 | 4.4 | M D |
| CVE-2023-20991 | In btm_ble_process_periodic_adv_sync_lost_evt of ble_scanner_hci_interface.cc , there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255305114 | 4.4 | M D |
| CVE-2023-21014 | In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029326 | 4.4 | M D |
| CVE-2023-21013 | In forceStaDisconnection of hostapd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256818945 | 4.4 | M D |
| CVE-2023-20984 | In ParseBqrLinkQualityEvt of btif_bqr.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242993878 | 4.4 | M D |
| CVE-2023-20983 | In btm_ble_rand_enc_complete of btm_ble.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569449 | 4.4 | M D |
| CVE-2023-20982 | In btm_read_tx_power_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568083 | 4.4 | M D |
| CVE-2023-21048 | In handleEvent of nan.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259304053References: N/A | 4.4 | M D |
| CVE-2023-28708 | When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0.-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. | 4.3 | M D |
| CVE-2023-25688 | IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247606. | 4.3 | M D |
| CVE-2023-25196 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation Apache Fineract. Authorized users may be able to change or add data in certain components. This issue affects Apache Fineract: from 1.4 through 1.8.2. | 4.3 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20903 | This disclosure regards a vulnerability related to UAA refresh tokens and external identity providers.Assuming that an external identity provider is linked to the UAA, a refresh token is issued to a client on behalf of a user from that identity provider, the administrator of the UAA deactivates the identity provider from the UAA. It is expected that the UAA would reject a refresh token during a refresh token grant, but it does not (hence the vulnerability). It will continue to issue access tokens to request presenting such refresh tokens, as if the identity provider was still active. As a result, clients with refresh tokens issued through the deactivated identity provider would still have access to Cloud Foundry resources until their refresh token expires (which defaults to 30 days). | 4.3 | M D |
| CVE-2023-0498 | The WP Education WordPress plugin before 1.2.7 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-1681 | A vulnerability, which was classified as problematic, was found in Xunrui CMS 4.61. Affected is an unknown function of the file /config/myfield/test.php. The manipulation leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-224238 is the identifier assigned to this vulnerability. | 4.3 | M D |
| CVE-2022-45634 | An issue discovered in MEGAFEIS, BOFEI DBD+ Application for IOS & Android v1.4.4 allows authenticated attacker to gain access to sensitive account information | 4.3 | M D |
| CVE-2023-1089 | The Coupon Zen WordPress plugin before 1.0.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-1088 | The WP Plugin Manager WordPress plugin before 1.1.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-1086 | The Preview Link Generator WordPress plugin before 1.0.4 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0505 | The Ever Compare WordPress plugin through 1.2.3 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0504 | The HT Politic WordPress plugin before 2.3.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0503 | The Free WooCommerce Theme 99fy Extension WordPress plugin before 1.2.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0499 | The QuickSwish WordPress plugin before 1.1.0 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0497 | The HT Portfolio WordPress plugin before 1.1.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0496 | The HT Event WordPress plugin before 1.4.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0495 | The HT Slider For Elementor WordPress plugin before 1.4.0 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0484 | The Contact Form 7 Widget For Elementor Page Builder & Gutenberg Blocks WordPress plugin before 1.1.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-0467 | The WP Dark Mode WordPress plugin before 4.0.8 does not properly sanitize the style parameter in shortcodes before using it to load a PHP template. This leads to Local File Inclusion on servers where non-existent directories may be traversed, or when chained with another vulnerability allowing arbitrary directory creation. | 4.3 | M D |
| CVE-2022-41354 | An access control issue in Argo CD v2.4.12 and below allows unauthenticated attackers to enumerate existing applications. | 4.3 | M D |
| CVE-2023-1087 | The WC Sales Notification WordPress plugin before 1.2.3 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack | 4.3 | M D |
| CVE-2023-22251 | Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and earlier) are affected by an Incorrect Authorization vulnerability. A low-privileged authenticated attacker could leverage this vulnerability to achieve minor information disclosure. | 4.3 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-20059 | A vulnerability in the implementation of the Cisco Network Plug-and-Play (PnP) agent of Cisco DNA Center could allow an authenticated, remote attacker to view sensitive information in clear text. The attacker must have valid low-privileged user credentials. This vulnerability is due to improper role-based access control (RBAC) with the integration of PnP. An attacker could exploit this vulnerability by authenticating to the device and sending a query to an internal API. A successful exploit could allow the attacker to view sensitive information in clear text, which could include configuration files. | 4.3 | M D |
| CVE-2023-1402 | The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. | 4.3 | M D |
| CVE-2023-28334 | Authenticated users were able to enumerate other users' names via the learning plans page. | 4.3 | M D |
| CVE-2023-28336 | Insufficient filtering of grade report history made it possible for teachers to access the names of users they could not otherwise access. | 4.3 | M D |
| CVE-2022-40208 | In Moodle, insufficient limitations in some quiz web services made it possible for students to bypass sequential navigation during a quiz attempt. | 4.3 | M D |
| CVE-2023-28630 | GoCD is an open source continuous delivery server. In GoCD versions from 20.5.0 and below 23.1.0, if the server environment is not correctly configured by administrators to provide access to the relevant PostgreSQL or MySQL backup tools, the credentials for database access may be unintentionally leaked to admin alerts on the GoCD user interface. The vulnerability is triggered only if the GoCD server host is misconfigured to have backups enabled, but does not have access to the `pg_dump` or `mysqldump` utility tools to backup the configured database type (PostgreSQL or MySQL respectively). In such cases, failure to launch the expected backup utility reports the shell environment used to attempt to launch in the server admin alert, which includes the plaintext database password supplied to the configured tool. This vulnerability does not affect backups of the default on-disk H2 database that GoCD is configured to use. This issue has been addressed and fixed in GoCD 23.1.0. Users are advised to upgrade. Users unable to upgrade may disable backups, or administrators should ensure that the required `pg_dump` (PostgreSQL) or `mysqldump` (MySQL) binaries are available on the GoCD server when backups are triggered. | 4.2 | M D |
| CVE-2023-25820 | Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10, when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available. | 4.2 | M D |
| CVE-2023-28443 | Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 9.23.3, the `directus_refresh_token` is not redacted properly from the log outputs and can be used to impersonate users without their permission. This issue is patched in version 9.23.3. | 4.2 | M D |
| CVE-2022-1230 | This vulnerability allows local attackers to execute arbitrary code on affected installations of Samsung Galaxy S21 prior to 4.5.40.5 phones. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of redirections. An attacker can force a redirection to a site that serves malicious content. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the current user. Was ZDI-CAN-15918. | 3.9 | M D |
| CVE-2023-28858 | redis-py before 4.5.3 leaves a connection open after canceling an async Redis command at an inopportune time, and can send response data to the client of an unrelated request in an off-by-one manner. NOTE: this CVE Record was initially created in response to reports about ChatGPT, and 4.3.6, 4.4.3, and 4.5.3 were released (changing the behavior for pipeline operations); however, please see CVE-2023-28859 about addressing data leakage across AsyncIO connections in general. | 3.7 | M D |
| CVE-2023-1593 | A vulnerability, which was classified as problematic, has been found in SourceCodester Automatic Question Paper Generator System 1.0. This issue affects some unknown processing of the file classes/Master.php?f=save_class. The manipulation of the argument description leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-223661 was assigned to this vulnerability. | 3.5 | M D |
| CVE-2023-1573 | A vulnerability was found in DataGear up to 1.11.1 and classified as problematic. This issue affects some unknown processing of the component Graph Dataset Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.12.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-223565 was assigned to this vulnerability. | 3.5 | M D |
| CVE-2023-1635 | A vulnerability was found in OTCMS 6.72. It has been declared as problematic. Affected by this vulnerability is the function AutoRun of the file apiRun.php. The manipulation of the argument mode leads to cross site scripting. The attack can be launched remotely. The identifier VDB-224017 was assigned to this vulnerability. | 3.5 | M D |
| CVE-2023-1609 | A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been rated as problematic. This issue affects the function save of the file /api/admin/store/product/save. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223739. | 3.5 | M D |
| CVE-2023-1569 | A vulnerability classified as problematic was found in SourceCodester E-Commerce System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/user/controller.php?action=edit. The manipulation of the argument U_NAME with the input <script>alert('1')</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223561 was assigned to this vulnerability. | 3.5 | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2023-1616 | A vulnerability was found in XiaoBingBy TeaCMS up to 2.0.2. It has been classified as problematic. Affected is an unknown function of the component Article Title Handler. The manipulation with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223800. | 3.5 | M D |
| CVE-2023-1567 | A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/assign/assign.php. The manipulation of the argument sid leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223559. | 3.5 | M D |
| CVE-2023-1565 | A vulnerability was found in FeiFeiCMS 2.7.130201. It has been classified as problematic. This affects an unknown part of the file \Public\system\slide_add.html of the component Extension Tool. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223557 was assigned to this vulnerability. | 3.5 | M D |
| CVE-2023-25817 | Nextcloud server is an open source, personal cloud implementation. In versions from 24.0.0 and before 24.0.9 a user could escalate their permissions to delete files they were not supposed to deletable but only viewed or downloaded. This issue has been addressed andit is recommended that the Nextcloud Server is upgraded to 24.0.9. There are no known workarounds for this vulnerability. | 3.5 | M D |
| CVE-2023-1613 | A vulnerability has been found in Rebuild up to 3.2.3 and classified as problematic. This vulnerability affects unknown code of the file /feeds/post/publish. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-223744. | 3.5 | M D |
| CVE-2023-1562 | Mattermost fails to check the "Show Full Name" setting when rendering the result for the /plugins/focalboard/api/v2/users API call, allowing an attacker to learn the full name of a board owner. | 3.5 | M D |
| CVE-2016-15030 | A vulnerability classified as problematic has been found in Arno0x TwoFactorAuth. This affects an unknown part of the file login/login.php. The manipulation of the argument from leads to open redirect. It is possible to initiate the attack remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 8549ad3cf197095f783643e41333586d6a4d0e54. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-223803. | 3.5 | M D |
| CVE-2023-1568 | A vulnerability classified as problematic has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file /admin/reports/index.php of the component GET Parameter Handler. The manipulation of the argument date_to leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223560. | 3.5 | M D |
| CVE-2023-1513 | A flaw was found in KVM. When calling the KVM_GET_DEBUGREGS ioctl, on 32-bit systems, there might be some uninitialized portions of the kvm_debugregs structure that could be copied to userspace, causing an information leak. | 3.3 | M D |
| CVE-2023-1075 | A flaw was found in the Linux Kernel. The tls_is_tx_ready() incorrectly checks for list emptiness, potentially accessing a type confused entry to the list_head, leaking the last byte of the confused field that overlaps with rec->tx_ready. | 3.3 | M D |
| CVE-2023-1176 | Absolute Path Traversal in GitHub repository mlflow/mlflow prior to 2.2.2. | 3.3 | M D |
| CVE-2023-1570 | A vulnerability, which was classified as problematic, has been found in syoyo tinydng. Affected by this issue is the function __interceptor_memcpy of the file tiny_dng_loader.h. The manipulation leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. It is recommended to apply a patch to fix this issue. VDB-223562 is the identifier assigned to this vulnerability. | 3.3 | M D |
| CVE-2023-1560 | A vulnerability, which was classified as problematic, has been found in TinyTIFF 3.0.0.0. This issue affects some unknown processing of the file tinytiffreader.c of the component File Handler. The manipulation leads to buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-223553 was assigned to this vulnerability. | 2.8 | M D |
| CVE-2022-39043 | Juiker app stores debug logs which contains sensitive information to mobile external storage. An unauthenticated physical attacker can access these files to acquire partial user information such as personal contacts. | 2.4 | M D |
| CVE-2021-3923 | A flaw was found in the Linux kernel's implementation of RDMA over infiniband. An attacker with a privileged local account can leak kernel stack information when issuing commands to the /dev/infiniband/rdma_cm device node. While this access is unlikely to leak sensitive user information, it can be further used to defeat existing kernel protection mechanisms. | 2.3 | M D |
| CVE-2023-1572 | A vulnerability has been found in DataGear up to 1.11.1 and classified as problematic. This vulnerability affects unknown code of the component Plugin Handler. The manipulation leads to cross site scripting. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 1.12.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-223564. | 2.0 | M D |
| CVE-2020-12382 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12383 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2020-24449 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24459 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24461 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24463 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8748 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24465 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24466 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24467 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8728 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24464 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24468 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2023-1622 | 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 | M D |
| CVE-2020-24476 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24483 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8727 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8735 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24469 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24479 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24478 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2020-24477 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24470 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24471 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12379 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24472 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12381 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2023-27655 | Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2019-9587. Reason: This record is a reservation duplicate of CVE-2019-9587. Notes: All CVE users should reference CVE-2019-9587 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage. | N/A | M D |
| CVE-2020-12378 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8762 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2023-24367 | 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 | M D |
| CVE-2023-1632 | Rejected reason: ** REJECT ** 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: Vendor identified that the vulnerability does not exist within the product, but merely with this particular on premise customer's implementation. | N/A | M D |
| CVE-2022-3938 | 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 | M D |
| CVE-2022-46750 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-46749 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-46748 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-46747 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2023-1659 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. | N/A | M D |
| CVE-2022-46746 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-46745 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-46744 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2023-24787 | Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-24685. Reason: This record is a duplicate of CVE-2023-24685. Notes: All CVE users should reference CVE-2023-24685 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage. | N/A | M D |
| CVE-2021-3099 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none. | N/A | M D |
| CVE-2021-3091 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none. | N/A | M D |
| CVE-2020-8726 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12348 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0509 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0552 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0579 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0580 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0582 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0585 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0589 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12298 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12305 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12340 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12341 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12342 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-12343 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2020-12344 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-0581 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2022-40541 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40542 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40593 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40569 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40570 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40571 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40572 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40573 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40574 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40575 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40576 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40577 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40578 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40579 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40580 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40581 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40582 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-40583 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40584 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40585 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40586 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40587 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40588 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40589 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40590 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40591 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40568 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40567 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40566 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40553 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40543 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40544 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40545 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40546 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40547 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40548 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-40549 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40550 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40551 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40552 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40554 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40565 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40555 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40556 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40557 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40558 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40559 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40560 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40561 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40562 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40563 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40564 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40592 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40594 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2020-24487 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2022-40595 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2020-24523 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24522 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24521 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24544 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24520 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24545 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24519 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24518 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24517 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24546 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24547 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8668 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8673 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8686 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8697 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8699 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24510 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-8724 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2020-8725 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24508 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24499 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2023-22608 | 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 | M D |
| CVE-2020-24488 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24524 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24526 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2023-1648 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-0326. Reason: This candidate is a duplicate of CVE-2023-0326. Notes: All CVE users should reference CVE-2023-0326 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage. | N/A | M D |
| CVE-2020-24534 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2022-40596 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40597 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40598 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40599 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40600 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2022-40601 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none. | N/A | M D |
| CVE-2020-24538 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24537 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24536 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24535 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |

| CVE Number | Description | Base Score | R |
|---|---|---|---|
| CVE-2020-24533 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24543 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24539 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24532 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24531 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24540 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24530 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24529 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24541 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24528 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24527 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24542 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |
| CVE-2020-24484 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none. | N/A | M D |