SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 22 February 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-2023-22578 | Due to improper artibute filtering in the sequalize js library, can a attacker peform SQL injections. | 10.0 | More Details |
| CVE-2023-25765 | In Jenkins Email Extension Plugin 2.93 and earlier, templates defined inside a folder were not subject to Script Security protection, allowing attackers able to define email templates in folders to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM. | 9.9 | More Details |
| CVE-2023-22579 | Due to improper parameter filtering in the sequalize js library, can a attacker peform injection. | 9.9 | More Details |
| CVE-2023-26092 | Liima before 1.17.28 allows server-side template injection. | 9.8 | More Details |
| CVE-2021-32163 | Authentication vulnerability in MOSN v.0.23.0 allows attacker to escalate privileges via case-sensitive JWT authorization. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-33226 | Buffer Overflow vulnerability in Saltstack v.3003 and before allows attacker to execute arbitrary code via the func variable in salt/salt/modules/status.py file. NOTE: this is disputed by third parties because an attacker cannot influence the eval input | 9.8 | More Details |
| CVE-2021-33391 | An issue in HTACG HTML Tidy v5.7.28 allows attacker to execute arbitrary code via the -g option of the CleanNode() function in gdoc.c. | 9.8 | More Details |
| CVE-2021-33948 | SQL injection vulnerability in FantasticLBP Hotels Server v1.0 allows attacker to execute arbitrary code via the username parameter. | 9.8 | More Details |
| CVE-2021-33949 | An issue in FeMiner WMS v1.1 allows attackers to execute arbitrary code via the filename parameter and the exec function. | 9.8 | More Details |
| CVE-2021-34182 | An issue in ttyd v.1.6.3 allows attacker to execute arbitrary code via default configuration permissions. | 9.8 | More Details |
| CVE-2021-35261 | File Upload Vulnerability in Yupoxion BearAdmin before commit 10176153528b0a914eb4d726e200fd506b73b075 allows attacker to execute arbitrary remote code via the Upfile function of the extend/tools/Ueditor endpoint. | 9.8 | More Details |
| CVE-2023-23279 | Canteen Management System 1.0 is vulnerable to SQL Injection via /php_action/getOrderReport.php. | 9.8 | More Details |
| CVE-2022-40021 | QVidium Technologies Amino A140 (prior to firmware version 1.0.0-283) was discovered to contain a command injection vulnerability. | 9.8 | More Details |
| CVE-2023-23064 | TOTOLINK A720R V4.1.5cu.532_ B20210610 is vulnerable to Incorrect Access Control. | 9.8 | More Details |
| CVE-2022-48328 | app/Controller/Component/IndexFilterComponent.php in MISP before 2.4.167 mishandles ordered_url_params and additional_delimiters. | 9.8 | More Details |
| CVE-2022-48329 | MISP before 2.4.166 unsafely allows users to use the order parameter, related to app/Model/Attribute.php, app/Model/GalaxyCluster.php, app/Model/Workflow.php, and app/Plugin/Assets/models/behaviors/LogableBehavior.php. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-26093 | Liima before 1.17.28 allows Hibernate query language (HQL) injection, related to colToSort in the deployment filter. | 9.8 | More Details |
| CVE-2020-29168 | SQL Injection vulnerability in Projectworlds Online Doctor Appointment Booking System, allows attackers to gain sensitive information via the q parameter to the getuser.php endpoint. | 9.8 | More Details |
| CVE-2023-25613 | An LDAP Injection vulnerability exists in the LdapIdentityBackend of Apache Kerby before 2.0.3. | 9.8 | More Details |
| CVE-2023-25805 | versionn, software for changing version information across multiple files, has a command injection vulnerability in all versions prior to version 1.1.0. This issue is patched in version 1.1.0. | 9.8 | More Details |
| CVE-2022-48337 | GNU Emacs through 28.2 allows attackers to execute commands via shell metacharacters in the name of a source-code file, because lib-src/etags.c uses the system C library function in its implementation of the etags program. For example, a victim may use the "etags -u *" command (suggested in the etags documentation) in a situation where the current working directory has contents that depend on untrusted input. | 9.8 | More Details |
| CVE-2023-23452 | Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. | 9.8 | More Details |
| CVE-2023-23453 | Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. | 9.8 | More Details |
| CVE-2023-0232 | The ShopLentor WordPress plugin before 2.5.4 unserializes user input from cookies in order to track viewed products and user data, which could lead to PHP Object Injection. | 9.8 | More Details |
| CVE-2022-45564 | SQL Injection vulnerability in znfit Home improvement ERP management system V50_20220207,v42 allows attackers to execute arbitrary sql commands via the userCode parameter to the wechat applet. | 9.8 | More Details |
| CVE-2022-45677 | SQL Injection Vulnerability in tanujpatra228 Tution Management System (TMS) via the email parameter to processes/student_login.process.php. | 9.8 | More Details |
| CVE-2023-24184 | TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-22920 | A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could leverage this vulnerability to access an affected device using Telnet. | 9.8 | More Details |
| CVE-2022-46637 | Prolink router PRS1841 was discovered to contain hardcoded credentials for its Telnet and FTP services. | 9.8 | More Details |
| CVE-2023-25158 | GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. | 9.8 | More Details |
| CVE-2023-24320 | An access control issue in Axcora POS #0~gitf77ec09 allows unauthenticated attackers to execute arbitrary commands via unspecified vectors. | 9.8 | More Details |
| CVE-2023-25157 | GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatements* setting to mitigate the ``FeatureId`` misuse. | 9.8 | More Details |
| CVE-2022-47986 | IBM Aspera Faspex 4.4.2 Patch Level 1 and earlier could allow a remote attacker to execute arbitrary code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system. The obsolete API call was removed in Faspex 4.4.2 PL2. IBM X-Force ID: 243512. | 9.8 | More Details |
| CVE-2022-40032 | SQL Injection vulnerability in Simple Task Managing System version 1.0 in login.php in 'username' and 'password' parameters, allows attackers to execute arbitrary code and gain sensitive information. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-46892 | In Ampere AltraMax and Ampere Altra before 2.10c, improper access controls allows the OS to reinitialize a disabled root complex. | 9.8 | More Details |
| CVE-2023-24238 | TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the city parameter at setting/delStaticDhcpRules. | 9.8 | More Details |
| CVE-2023-22807 | LS ELECTRIC XBC-DN32U with operating system version 01.80 does not properly control access to the PLC over its internal XGT protocol. An attacker could control and tamper with the PLC by sending the packets to the PLC over its XGT protocol. | 9.8 | More Details |
| CVE-2023-23461 | Libpeconv – access violation, before commit b076013 (30/11/2022). | 9.8 | More Details |
| CVE-2023-23462 | Libpeconv – integer overflow, before commit 75b1565 (30/11/2022). | 9.8 | More Details |
| CVE-2023-22855 | Kardex Mlog MCC 5.7.12+0-a203c2a213-master allows remote code execution. It spawns a web interface listening on port 8088. A user-controllable path is handed to a path-concatenation method (Path.Combine from .NET) without proper sanitisation. This yields the possibility of including local files, as well as remote files on SMB shares. If one provides a file with the extension .t4, it is rendered with the .NET templating engine mono/t4, which can execute code. | 9.8 | More Details |
| CVE-2020-21119 | SQL Injection vulnerability in Kliqqi-CMS 2.0.2 in admin/admin_update_module_widgets.php in recordIDValue parameter, allows attackers to gain escalated privileges and execute arbitrary code. | 9.8 | More Details |
| CVE-2020-21120 | SQL Injection vulnerability in file home\controls\cart.class.php in UQCMS 2.1.3, allows attackers execute arbitrary commands via the cookie_cart parameter to /index.php/cart/num. | 9.8 | More Details |
| CVE-2021-33304 | Double Free vulnerability in virtualsquare picoTCP v1.7.0 and picoTCP-NG v2.1 in modules/pico_fragments.c in function pico_fragments_reassemble, allows attackers to execute arbitrary code. | 9.8 | More Details |
| CVE-2022-40347 | SQL Injection vulnerability in Intern Record System version 1.0 in /intern/controller.php in 'phone', 'email', 'deptType' and 'name' parameters, allows attackers to execute arbitrary code and gain sensitive information. | 9.8 | More Details |
| CVE-2023-24236 | TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the province parameter at setting/delStaticDhcpRules. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-33925 | SQL Injection vulnerability in nitinparashar30 cms-corephp through commit bdabe52ef282846823bda102728a35506d0ec8f9 (May 19, 2021) allows unauthenticated attackers to gain escilated privledges via a crafted login. | 9.8 | More Details |
| CVE-2021-43529 | Thunderbird versions prior to 91.3.0 are vulnerable to the heap overflow described in CVE-2021-43527 when processing S/MIME messages. Thunderbird versions 91.3.0 and later will not call the vulnerable code when processing S/MIME messages that contain certificates with DER-encoded DSA or RSA-PSS signatures. | 9.8 | More Details |
| CVE-2022-39952 | A external control of file name or path in Fortinet FortiNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.7, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP request. | 9.8 | More Details |
| CVE-2023-24221 | LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/DeptMapper.xml. | 9.8 | More Details |
| CVE-2023-24220 | LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/RoleMapper.xml. | 9.8 | More Details |
| CVE-2023-24219 | LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/UserMapper.xml. | 9.8 | More Details |
| CVE-2023-24080 | A lack of rate limiting on the password reset endpoint of Chamberlain myQ v5.222.0.32277 (on iOS) allows attackers to compromise user accounts via a bruteforce attack. | 9.8 | More Details |
| CVE-2021-42756 | Multiple stack-based buffer overflow vulnerabilities [CWE-121] in the proxy daemon of FortiWeb 5.x all versions, 6.0.7 and below, 6.1.2 and below, 6.2.6 and below, 6.3.16 and below, 6.4 all versions may allow an unauthenticated remote attacker to achieve arbitrary code execution via specifically crafted HTTP requests. | 9.8 | More Details |
| CVE-2020-19825 | Cross Site Scripting (XSS) vulnerability in kevinpapst kimai2 1.30.0 in /src/Twig/Runtime/MarkdownExtension.php, allows attackers to gain escalated privileges. | 9.6 | More Details |
| CVE-2022-38375 | An improper authorization vulnerability [CWE-285] in Fortinet FortiNAC version 9.4.0 through 9.4.1 and before 9.2.6 allows an unauthenticated user to perform some administrative operations over the FortiNAC instance via crafted HTTP POST requests. | 9.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-46836 | PHP code injection in watolib auth.php and hosttags.php in Tribe29's Checkmk <= 2.1.0p10, Checkmk <= 2.0.0p27, and Checkmk <= 1.6.0p29 allows an attacker to inject and execute PHP code which will be executed upon request of the vulnerable component. | 9.1 | More Details |
| CVE-2022-3843 | In WAGO Unmanaged Switch (852-111/000-001) in firmware version 01 an undocumented configuration interface without authorization allows an remote attacker to read system information and configure a limited set of parameters. | 9.1 | More Details |
| CVE-2023-23465 | Media CP Media Control Panel latest version. CSRF possible through unspecified endpoint. | 9.1 | More Details |
| CVE-2023-23460 | Priority Web version 19.1.0.68, parameter manipulation on an unspecified end-point may allow authentication bypass. | 9.1 | More Details |
| CVE-2023-23459 | Priority Windows may allow Command Execution via SQL Injection using an unspecified method. | 9.1 | More Details |
| CVE-2022-43969 | Ricoh mp_c4504ex devices with firmware 1.06 mishandle credentials. | 9.1 | More Details |
| CVE-2023-22804 | LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication to create users on the PLC. This could allow an attacker to create and use an account with elevated privileges and take control of the device. | 9.1 | More Details |
| CVE-2023-0102 | LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication for its deletion command. This could allow an attacker to delete arbitrary files. | 9.1 | More Details |
| CVE-2023-23947 | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0-rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23, and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhitelist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields. | 9.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-42761 | A condition for session fixation vulnerability [CWE-384] in the session management of FortiWeb versions 6.4 all versions, 6.3.0 through 6.3.16, 6.2.0 through 6.2.6, 6.1.0 through 6.1.2, 6.0.0 through 6.0.7, 5.9.0 through 5.9.1 may allow a remote, unauthenticated attacker to infer the session identifier of other users and possibly usurp their session. | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-29557 | LexisNexis Firco Compliance Link 3.7 allows CSRF. | 8.8 | More Details |
| CVE-2022-42735 | Improper Privilege Management vulnerability in Apache Software Foundation Apache ShenYu. ShenYu Admin allows low-privilege low-level administrators create users with higher privileges than their own. This issue affects Apache ShenYu: 2.5.0. Upgrade to Apache ShenYu 2.5.1 or apply patch https://github.com/apache/shenyu/pull/3958 https://github.com/apache/shenyu/pull/3958 . | 8.8 | More Details |
| CVE-2022-38867 | SQL Injection vulnerability in rttys versions 4.0.0, 4.0.1, and 4.0.2 in api.go, allows attackers to execute arbitrary code. | 8.8 | More Details |
| CVE-2022-38935 | An issue was discovered in NiterForum version 2.5.0-beta in /src/main/java/cn/niter/forum/api/SsoApi.java and /src/main/java/cn/niter/forum/controller/AdminController.java, allows attackers to gain escalated privileges. | 8.8 | More Details |
| CVE-2022-30303 | An improper neutralization of special elements used in an os command ('OS Command Injection') [CWE-78] in FortiWeb 7.0.0 through 7.0.1, 6.3.0 through 6.3.19, 6.4 all versions may allow an authenticated attacker to execute arbitrary shell code as `root` user via crafted HTTP requests. | 8.8 | More Details |
| CVE-2022-33869 | An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the management interface of FortiWAN 4.0.0 through 4.5.9 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. | 8.8 | More Details |
| CVE-2022-41334 | An improper neutralization of input during web page generation [CWE-79] vulnerability in FortiOS versions 7.0.0 to 7.0.7 and 7.2.0 to 7.2.3 may allow a remote, unauthenticated attacker to launch a cross site scripting (XSS) attack via the "redir" parameter of the URL seen when the "Sign in with FortiCloud" button is clicked. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-41335 | A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.10, FortiProxy version 7.2.0 through 7.2.1, 7.0.0 through 7.0.7 and before 2.0.10, FortiSwitchManager 7.2.0 and before 7.0.0 allows an authenticated attacker to read and write files on the underlying Linux system via crafted HTTP requests. | 8.8 | More Details |
| CVE-2022-36348 | Active debug code in some Intel (R) SPS firmware before version SPS_E5_04.04.04.300.0 may allow an authenticated user to potentially enable escalation of privilege via local access. | 8.8 | More Details |
| CVE-2023-25767 | A cross-site request forgery (CSRF) vulnerability in Jenkins Azure Credentials Plugin 253.v887e0f9e898b and earlier allows attackers to connect to an attacker-specified web server. | 8.8 | More Details |
| CVE-2023-0877 | Code Injection in GitHub repository froxlor/froxlor prior to 2.0.11. | 8.8 | More Details |
| CVE-2023-24078 | Real Time Logic FuguHub v8.1 and earlier was discovered to contain a remote code execution (RCE) vulnerability via the component /FuguHub/cmsdocs/. | 8.8 | More Details |
| CVE-2023-0882 | Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Kron Tech Single Connect on Windows allows Privilege Abuse. This issue affects Single Connect: 2.16. | 8.8 | More Details |
| CVE-2022-45701 | Arris TG2482A firmware through 9.1.103GEM9 allow Remote Code Execution (RCE) via the ping utility feature. | 8.8 | More Details |
| CVE-2023-0822 | The affected product DIAEnergie (versions prior to v1.9.03.001) contains improper authorization, which could allow an unauthorized user to bypass authorization and access privileged functionality. | 8.8 | More Details |
| CVE-2021-33926 | An issue in Plone CMS v. 5.2.4, 5.2.3, 5.2.2, 5.2.1, 5.2.0, 5.1rc2, 5.1rc1, 5.1b4, 5.1b3, 5.1b2, 5.1a2, 5.1a1, 5.1.7, 5.1.6, 5.1.5, 5.1.4, 5.1.2, 5.1.1 5.1, 5.0rc3, 5.0rc2, 5.0rc1, 5.0.9, 5.0.8, 5.0.7, 5.0.6, 5.0.5, 5.0.4, 5.0.3, 5.0.2, 5.0.10, 5.0.1, 5.0, 4.3.9, 4.3.8, 4.3.7, 4.3.6, 4.3.5, 4.3.4, 4.3.3, 4.3.20, 4 allows attacker to access sensitive information via the RSS feed protlet. | 8.8 | More Details |
| CVE-2021-34164 | Permissions vulnerability in LIZHIFAKA v.2.2.0 allows authenticated attacker to execute arbitrary commands via the set password function in the admin/index/email location. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-20803 | A vulnerability in the OLE2 file parser of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device.The vulnerability is due to incorrect use of the realloc function that may result in a double-free. An attacker could exploit this vulnerability by submitting a crafted OLE2 file to be scanned by ClamAV on the affected device. An exploit could allow the attacker to cause the ClamAV scanning process to crash, resulting in a denial of service condition. | 8.6 | More Details |
| CVE-2022-21163 | Improper access control in the Crypto API Toolkit for Intel(R) SGX before version 2.0 commit ID 91ee496 may allow an authenticated user to potentially enable escalation of privilege via local access. | 8.4 | More Details |
| CVE-2022-26843 | Insufficient visual distinction of homoglyphs presented to user in the Intel(R) oneAPI DPC++/C++ Compiler before version 2022.1 for Intel(R) oneAPI Toolkits before version 2022.2 may allow an unauthenticated user to potentially enable escalation of privilege via network access. | 8.3 | More Details |
| CVE-2022-25987 | Improper handling of Unicode encoding in source code to be compiled by the Intel(R) C++ Compiler Classic before version 2021.6 for Intel(R) oneAPI Toolkits before version 2022.2 may allow an unauthenticated user to potentially enable escalation of privilege via network access. | 8.3 | More Details |
| CVE-2023-0880 | Misinterpretation of Input in GitHub repository thorsten/phpmyfaq prior to 3.1.11. | 8.3 | More Details |
| CVE-2022-26343 | Improper access control in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. | 8.2 | More Details |
| CVE-2023-23923 | The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality. | 8.2 | More Details |
| CVE-2022-34153 | Improper initialization in the Intel(R) Battery Life Diagnostic Tool software before version 2.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access. | 8.2 | More Details |
| CVE-2022-36278 | Insufficient control flow management in the Intel(R) Battery Life Diagnostic Tool software before version 2.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access. | 8.2 | More Details |
| CVE-2021-3172 | An issue in Php-Fusion v9.03.90 fixed in v9.10.00 allows authenticated attackers to cause a Distributed Denial of Service via the Polling feature. | 8.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-23467 | Media CP Media Control Panel latest version. Reflected XSS possible through unspecified endpoint. | 8.1 | More Details |
| CVE-2023-23464 | Media CP Media Control Panel latest version. A Permissive Flash Cross-domain Policy may allow information disclosure. | 8.1 | More Details |
| CVE-2023-0919 | Missing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0. | 8.1 | More Details |
| CVE-2022-46303 | Command injection in SMS notifications in Tribe29 Checkmk <= 2.1.0p10, Checkmk <= 2.0.0p27, and Checkmk <= 1.6.0p29 allows an attacker with User Management permissions, as well as LDAP administrators in certain scenarios, to perform arbitrary commands within the context of the application's local permissions. | 8.0 | More Details |
| CVE-2023-23780 | A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via specifically crafted HTTP requests. | 8.0 | More Details |
| CVE-2023-21621 | FrameMaker 2020 Update 4 (and earlier), 2022 (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 | More Details |
| CVE-2023-22246 | Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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 | More Details |
| CVE-2023-22226 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are 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 | More Details |
| CVE-2023-22244 | Adobe Premiere Rush version 2.6 (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 | More Details |
| CVE-2023-21619 | FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-21576 | Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2023-21622 | FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2023-22238 | After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2023-22243 | Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are 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 | More Details |
| CVE-2023-22239 | After Affects versions 23.1 (and earlier), 22.6.3 (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 | More Details |
| CVE-2023-22227 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2022-47506 | SolarWinds Platform was susceptible to the Directory Traversal Vulnerability. This vulnerability allows a local adversary with authenticated account access to edit the default configuration, enabling the execution of arbitrary commands. | 7.8 | More Details |
| CVE-2022-42455 | ASUS EC Tool driver (aka d.sys) 1beb15c90dcf7a5234ed077833a0a3e900969b60be1d04fcebce0a9f8994bdbb, as signed by ASUS and shipped with multiple ASUS software products, contains multiple IOCTL handlers that provide raw read and write access to port I/O and MSRs via unprivileged IOCTL calls. Local users can gain privileges. | 7.8 | More Details |
| CVE-2023-22237 | After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-22228 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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 | More Details |
| CVE-2023-22236 | Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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 | More Details |
| CVE-2023-22229 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2023-22230 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2023-21575 | Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2023-24483 | A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTEM on a Citrix Virtual Apps and Desktops Windows VDA. | 7.8 | More Details |
| CVE-2023-21574 | Photoshop version 23.5.3 (and earlier), 24.1 (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 | More Details |
| CVE-2023-24575 | Dell Multifunction Printer E525w Driver and Software Suite, versions prior to 1.047.2022, A05, contain a local privilege escalation vulnerability that could be exploited by malicious users to compromise the affected system | 7.8 | More Details |
| CVE-2022-30530 | Protection mechanism failure in the Intel(R) DSA software before version 22.4.26 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.8 | More Details |
| CVE-2023-20927 | In permissions of AndroidManifest.xml, there is a possible way to grant signature permissions 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-244216503 | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25602 | A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. | 7.8 | More Details |
| CVE-2023-23782 | A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. | 7.8 | More Details |
| CVE-2022-40080 | Stack overflow vulnerability in Aspire E5-475G 's BIOS firmware, in the FpGui module, a second call to GetVariable services allows local attackers to execute arbitrary code in the UEFI DXE phase and gain escalated privileges. | 7.8 | More Details |
| CVE-2023-0866 | Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3.0-DEV. | 7.8 | More Details |
| CVE-2022-36369 | Improper access control in some QATzip software maintained by Intel(R) before version 1.0.9 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.8 | More Details |
| CVE-2022-40683 | A double free in Fortinet FortiWeb version 7.0.0 through 7.0.3 may allows attacker to execute unauthorized code or commands via specially crafted commands | 7.8 | More Details |
| CVE-2023-22368 | Untrusted search path vulnerability in ELECOM Camera Assistant 1.00 and QuickFileDealer Ver.1.2.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. | 7.8 | More Details |
| CVE-2022-32972 | Infoblox BloxOne Endpoint for Windows through 2.2.7 allows DLL injection that can result in local privilege escalation. | 7.8 | More Details |
| CVE-2021-32142 | Buffer Overflow vulnerability in LibRaw linux/unix v0.20.0 allows attacker to escalate privileges via the LibRaw_buffer_datastream::gets(char*, int) in /src/libraw/src/libraw_datastream.cpp. | 7.8 | More Details |
| CVE-2022-48339 | An issue was discovered in GNU Emacs through 28.2. htmlfontify.el has a command injection vulnerability. In the hfy-istext-command function, the parameter file and parameter srcdir come from external input, and parameters are not escaped. If a file name or directory name contains shell metacharacters, code may be executed. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-26242 | afu_mmio_region_get_by_offset in drivers/fpga/dfl-afu-region.c in the Linux kernel through 6.1.12 has an integer overflow. | 7.8 | More Details |
| CVE-2022-27482 | A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiADC version 7.0.0 through 7.0.1, 6.2.0 through 6.2.2, 6.1.0 through 6.1.6, 6.0.x, 5.x.x allows attacker to execute arbitrary shell code as `root` via CLI commands. | 7.8 | More Details |
| CVE-2021-33983 | Buffer Overflow vulnerability in Dvidelabs flatcc v.0.6.0 allows local attacker to execute arbitrary code via the fltacc execution of the error_ref_sym function. | 7.8 | More Details |
| CVE-2023-24485 | Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the computer running Citrix Workspace app. | 7.8 | More Details |
| CVE-2023-22234 | Adobe Premiere Rush version 2.6 (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 | More Details |
| CVE-2023-25011 | PC settings tool Ver10.1.26.0 and earlier, PC settings tool Ver11.0.22.0 and earlier allows a attacker to write to the registry as administrator privileges with standard user privileges. | 7.8 | More Details |
| CVE-2022-29514 | Improper access control in the Intel(R) SUR software before version 2.4.8902 may allow an unauthenticated user to potentially enable escalation of privilege via network access. | 7.7 | More Details |
| CVE-2021-32846 | HyperKit is a toolkit for embedding hypervisor capabilities in an application. In versions 0.20210107, function `pci_vtsock_proc_tx` in `virtio-sock` can lead to to uninitialized memory use. In this situation, there is a check for the return value to be less or equal to `VTSOCK_MAXSEGS`, but that check is not sufficient because the function can return `-1` if it finds an error it cannot recover from. Moreover, the negative return value will be used by `iovec_pull` in a while condition that can further lead to more corruption because the function is not designed to handle a negative `iov_len`. This issue may lead to a guest crashing the host causing a denial of service and, under certain circumstance, memory corruption. This issue is fixed in commit af5eba2360a7351c08dfd9767d9be863a50ebaba. | 7.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32845 | HyperKit is a toolkit for embedding hypervisor capabilities in an application. In versions 0.20210107 and prior of HyperKit, the implementation of `qnotify` at `pci_vtrnd_notify` fails to check the return value of `vq_getchain`. This leads to `struct iovec iov;` being uninitialized and used to read memory in `len = (int) read(sc->vrsc_fd, iov.iov_base, iov.iov_len);` when an attacker is able to make `vq_getchain` fail. This issue may lead to a guest crashing the host causing a denial of service and, under certain circumstance, memory corruption. This issue is fixed in commit 41272a980197917df8e58ff90642d14dec8fe948. | 7.7 | More Details |
| CVE-2022-47372 | Stored cross-site scripting vulnerability in the Create event section in Pandora FMS Console v766 and lower. An attacker typically exploits this vulnerability by injecting XSS payloads on popular pages of a site or passing a link to a victim, tricking them into viewing the page that contains the stored XSS payload. | 7.6 | More Details |
| CVE-2022-21216 | Insufficient granularity of access control in out-of-band management in some Intel(R) Atom and Intel Xeon Scalable Processors may allow a privileged user to potentially enable escalation of privilege via adjacent network access. | 7.5 | More Details |
| CVE-2023-22803 | LS ELECTRIC XBC-DN32U with operating system version 01.80 is missing authentication to perform critical functions to the PLC. This could allow an attacker to change the PLC's mode arbitrarily. | 7.5 | More Details |
| CVE-2023-24807 | Undici is an HTTP/1.1 client for Node.js. Prior to version 5.19.1, the `Headers.set()` and `Headers.append()` methods are vulnerable to Regular Expression Denial of Service (ReDoS) attacks when untrusted values are passed into the functions. This is due to the inefficient regular expression used to normalize the values in the `headerValueNormalize()` utility function. This vulnerability was patched in v5.19.1. No known workarounds are available. | 7.5 | More Details |
| CVE-2023-0103 | If an attacker were to access memory locations of LS ELECTRIC XBC-DN32U with operating system version 01.80 that are outside of the communication buffer, the device stops operating. This could allow an attacker to cause a denial-of-service condition. | 7.5 | More Details |
| CVE-2022-32764 | Description: Race condition in the Intel(R) DSA software before version 22.4.26 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.5 | More Details |
| CVE-2021-33950 | An issue discovered in OpenKM v6.3.10 allows attackers to obtain sensitive information via the XMLTextExtractor function. | 7.5 | More Details |
| CVE-2021-32441 | SQL Injection vulnerability in Exponent-CMS v.2.6.0 fixed in 2.7.0 allows attackers to gain access to sensitive information via the selectValue function in the expConfig class. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25578 | Starlite is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to version 1.5.2, the request body parsing in `starlite` allows a potentially unauthenticated attacker to consume a large amount of CPU time and RAM. The multipart body parser processes an unlimited number of file parts and an unlimited number of field parts. This is a remote, potentially unauthenticated Denial of Service vulnerability. This vulnerability affects applications with a request handler that accepts a `Body(media_type=RequestEncodingType.MULTI_PART)`. The large amount of CPU time required for processing requests can block all available worker processes and significantly delay or slow down the processing of legitimate user requests. The large amount of RAM accumulated while processing requests can lead to Out-Of-Memory kills. Complete DoS is achievable by sending many concurrent multipart requests in a loop. Version 1.51.2 contains a patch for this issue. | 7.5 | More Details |
| CVE-2022-40016 | Use After Free (UAF) vulnerability in ireader media-server before commit 3e0f63f1d3553f75c7d4eb32fa7c7a1976a9ff84 in librtmp, allows attackers to cause a denial of service. | 7.5 | More Details |
| CVE-2023-24580 | An issue was discovered in the Multipart Request Parser in Django 3.2 before 3.2.18, 4.0 before 4.0.10, and 4.1 before 4.1.7. Passing certain inputs (e.g., an excessive number of parts) to multipart forms could result in too many open files or memory exhaustion, and provided a potential vector for a denial-of-service attack. | 7.5 | More Details |
| CVE-2023-22806 | LS ELECTRIC XBC-DN32U with operating system version 01.80 transmits sensitive information in cleartext when communicating over its XGT protocol. This could allow an attacker to gain sensitive information such as user credentials. | 7.5 | More Details |
| CVE-2023-25191 | AMI MegaRAC SPX devices allow Password Disclosure through Redfish. The fixed versions are SPx_12-update-7.00 and SPx_13-update-5.00. | 7.5 | More Details |
| CVE-2022-47703 | TIANJIE CPE906-3 is vulnerable to password disclosure. This is present on Software Version WEB5.0_LCD_20200513, Firmware Version MV8.003, and Hardware Version CPF906-V5.0_LCD_20200513. | 7.5 | More Details |
| CVE-2020-6817 | bleach.clean behavior parsing style attributes could result in a regular expression denial of service (ReDoS). Calls to bleach.clean with an allowed tag with an allowed style attribute are vulnerable to ReDoS. For example, bleach.clean(..., attributes={'a': ['style']}). | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25171 | Kiwi TCMS, an open source test management system, does not impose rate limits in versions prior to 12.0. This makes it easier to attempt denial-of-service attacks against the Password reset page. An attacker could potentially send a large number of emails if they know the email addresses of users in Kiwi TCMS. Additionally that may strain SMTP resources. Users should upgrade to v12.0 or later to receive a patch. As potential workarounds, users may install and configure a rate-limiting proxy in front of Kiwi TCMS and/or configure rate limits on their email server when possible. | 7.5 | More Details |
| CVE-2023-25156 | Kiwi TCMS, an open source test management system, does not impose rate limits in versions prior to 12.0. This makes it easier to attempt brute-force attacks against the login page. Users should upgrade to v12.0 or later to receive a patch. As a workaround, users may install and configure a rate-limiting proxy in front of Kiwi TCMS. | 7.5 | More Details |
| CVE-2022-35729 | Out of bounds read in firmware for OpenBMC in some Intel(R) platforms before version 0.72 may allow unauthenticated user to potentially enable denial of service via network access. | 7.5 | More Details |
| CVE-2023-25653 | node-jose is a JavaScript implementation of the JSON Object Signing and Encryption (JOSE) for web browsers and node.js-based servers. Prior to version 2.2.0, when using the non-default "fallback" crypto back-end, ECC operations in `node-jose` can trigger a Denial-of-Service (DoS) condition, due to a possible infinite loop in an internal calculation. For some ECC operations, this condition is triggered randomly; for others, it can be triggered by malicious input. The issue has been patched in version 2.2.0. Since this issue is only present in the "fallback" crypto implementation, it can be avoided by ensuring that either WebCrypto or the Node `crypto` module is available in the JS environment where `node-jose` is being run. | 7.5 | More Details |
| CVE-2023-26081 | In Epiphany (aka GNOME Web) through 43.0, untrusted web content can trick users into exfiltrating passwords, because autofill occurs in sandboxed contexts. | 7.5 | More Details |
| CVE-2021-32848 | Octobox is software for managing GitHub notifications. Prior to pull request (PR) 2807, a user of the system can provide a specifically crafted search query string that will trigger a ReDoS vulnerability. This issue is fixed in PR 2807. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25657 | Nautobot is a Network Source of Truth and Network Automation Platform. All users of Nautobot versions earlier than 1.5.7 are impacted by a remote code execution vulnerability. Nautobot did not properly sandbox Jinja2 template rendering. In Nautobot 1.5.7 has enabled sandboxed environments for the Jinja2 template engine used internally for template rendering for the following objects: `extras.ComputedField`, `extras.CustomLink`, `extras.ExportTemplate`, `extras.Secret`, `extras.Webhook`. While no active exploits of this vulnerability are known this change has been made as a preventative measure to protect against any potential remote code execution attacks utilizing maliciously crafted template code. This change forces the Jinja2 template engine to use a `SandboxedEnvironment` on all new installations of Nautobot. This addresses any potential unsafe code execution everywhere the helper function `nautobot.utilities.utils.render_jinja2` is called. Additionally, the documentation that had previously suggesting the direct use of `jinja2.Template` has been revised to suggest `render_jinja2`. Users are advised to upgrade to Nautobot 1.5.7 or newer. For users that are unable to upgrade to the latest release of Nautobot, you may add the following setting to your `nautobot_config.py` to apply the sandbox environment enforcement: `TEMPLATES[1]["OPTIONS"]["environment"] = "jinja2.sandbox.SandboxedEnvironment"` After applying this change, you must restart all Nautobot services, including any Celery worker processes. **Note:** *Nautobot specifies two template engines by default, the first being “django” for the Django built-in template engine, and the second being “jinja” for the Jinja2 template engine. This recommended setting will update the second item in the list of template engines, which is the Jinja2 engine.* For users that are unable to immediately update their configuration such as if a Nautobot service restart is too disruptive to operations, access to provide custom Jinja2 template values may be mitigated using permissions to restrict “change” (write) actions to the affected object types listed in the first section. **Note:** *This solution is intended to be stopgap until you can successfully update your `nautobot_config.py` or upgrade your Nautobot instance to apply the sandboxed environment enforcement.* | 7.5 | More Details |
| CVE-2023-24329 | An issue in the urllib.parse component of Python before 3.11.4 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters. | 7.5 | More Details |
| CVE-2022-44216 | Gnuboard 5.5.4 and 5.5.5 is vulnerable to Insecure Permissions. An attacker can change password of all users without knowing victim's original password. | 7.5 | More Details |
| CVE-2022-45546 | Information Disclosure in Authentication Component of ScreenCheck BadgeMaker 2.6.2.0 application allows internal attacker to obtain credentials for authentication via network sniffing. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-31394 | Hyperium Hyper before 0.14.19 does not allow for customization of the max_header_list_size method in the H2 third-party software, allowing attackers to perform HTTP2 attacks. | 7.5 | More Details |
| CVE-2023-25656 | notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The problem has been patched in the release v1.0.0-rc.3. Some workarounds are available. Users can review their own trust policy file and check if the identity string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`. | 7.5 | More Details |
| CVE-2023-0662 | In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the affected server by exhausting CPU resources or disk space. | 7.5 | More Details |
| CVE-2023-25570 | Apollo is a configuration management system. Prior to version 2.1.0, there are potential security issues if users expose apollo-configservice to the internet, which is not recommended. This is because there is no authentication feature enabled for the built-in eureka service. Malicious hackers may access eureka directly to mock apollo-configservice and apollo-adminservice. Login authentication for eureka was added in version 2.1.0. As a workaround, avoid exposing apollo-configservice to the internet. | 7.5 | More Details |
| CVE-2023-24998 | Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option (FileUploadBase#setFileCountMax) is not enabled by default and must be explicitly configured. | 7.5 | More Details |
| CVE-2023-24498 | An uspecified endpoint in the web server of the switch does not properly authenticate the user identity, and may allow downloading a config page with the password to the switch in clear text. | 7.5 | More Details |
| CVE-2022-26837 | Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. | 7.5 | More Details |
| CVE-2022-30539 | Use after free in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. | 7.5 | More Details |
| CVE-2022-48340 | In Gluster GlusterFS 11.0, there is an xlators/cluster/dht/src/dht-common.c dht_setxattr_mds_cbk use-after-free. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-47508 | Customers who had configured their polling to occur via Kerberos did not expect NTLM Traffic on their environment, but since we were querying for data via IP address this prevented us from utilizing Kerberos. | 7.5 | More Details |
| CVE-2023-0568 | In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. | 7.5 | More Details |
| CVE-2022-32231 | Improper initialization in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. | 7.5 | More Details |
| CVE-2022-25992 | Insecure inherited permissions in the Intel(R) oneAPI Toolkits oneapi-cli before version 0.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.5 | More Details |
| CVE-2023-24960 | IBM InfoSphere Information Server 11.7 could 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: 246333 | 7.5 | More Details |
| CVE-2021-34117 | SQL Injection vulnerability in SEO Panel 4.9.0 in api/user.api.php in function getUserName in the username parameter, allows attackers to gain sensitive information. | 7.5 | More Details |
| CVE-2021-38239 | SQL Injection vulnerability in dataease before 1.2.0, allows attackers to gain sensitive information via the orders parameter to /api/sys_msg/list/1/10. | 7.5 | More Details |
| CVE-2023-26253 | In Gluster GlusterFS 11.0, there is an xlators/mount/fuse/src/fuse-bridge.c notify stack-based buffer over-read. | 7.5 | More Details |
| CVE-2023-26249 | Knot Resolver before 5.6.0 enables attackers to consume its resources, launching amplification attacks and potentially causing a denial of service. Specifically, a single client query may lead to a hundred TCP connection attempts if a DNS server closes connections without providing a response. | 7.5 | More Details |
| CVE-2023-0860 | Improper Restriction of Excessive Authentication Attempts in GitHub repository modoboa/modoboa-installer prior to 2.0.4. | 7.5 | More Details |
| CVE-2022-40678 | An insufficiently protected credentials in Fortinet FortiNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.7, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7 may allow a local attacker with database access to recover user passwords. | 7.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-33964 | Improper input validation in the Intel(R) SUR software before version 2.4.8902 may allow an unauthenticated user to potentially enable escalation of privilege via network access. | 7.4 | More Details |
| CVE-2023-22377 | Improper restriction of XML external entity reference (XXE) vulnerability exists in tsClinical Define.xml Generator all versions (v1.0.0 to v1.4.0) and tsClinical Metadata Desktop Tools Version 1.0.3 to Version 1.1.0. If this vulnerability is exploited, an attacker may obtain an arbitrary file which meets a certain condition by reading a specially crafted XML file. | 7.4 | More Details |
| CVE-2023-0361 | A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By recovering the secret from the ClientKeyExchange message, the attacker would be able to decrypt the application data exchanged over that connection. | 7.4 | More Details |
| CVE-2022-33892 | Path traversal in the Intel(R) Quartus Prime Pro and Standard edition software may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.3 | More Details |
| CVE-2022-36397 | Incorrect default permissions in the software installer for some Intel(R) QAT drivers for Linux before version 4.17 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.3 | More Details |
| CVE-2022-39954 | An improper restriction of xml external entity reference in Fortinet FortiNAC version 9.4.0 through 9.4.1, FortiNAC version 9.2.0 through 9.2.7, FortiNAC version 9.1.0 through 9.1.8, FortiNAC version 8.8.0 through 8.8.11, FortiNAC version 8.7.0 through 8.7.6, FortiNAC version 8.6.0 through 8.6.5, FortiNAC version 8.5.0 through 8.5.4, FortiNAC version 8.3.7 allows attacker to read arbitrary files or trigger a denial of service via specifically crafted XML documents. | 7.3 | More Details |
| CVE-2023-0905 | A vulnerability classified as critical has been found in SourceCodester Employee Task Management System 1.0. Affected is an unknown function of the file changePasswordForEmployee.php. The manipulation leads to improper authentication. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221454 is the identifier assigned to this vulnerability. | 7.3 | More Details |
| CVE-2022-33902 | Insufficient control flow management in the Intel(R) Quartus Prime Pro and Standard edition software may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0906 | A vulnerability classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. Affected by this vulnerability is the function delete_category of the file ajax.php of the component POST Parameter Handler. The manipulation leads to missing authentication. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-221455. | 7.3 | More Details |
| CVE-2022-48338 | An issue was discovered in GNU Emacs through 28.2. In ruby-mode.el, the ruby-find-library-file function has a local command injection vulnerability. The ruby-find-library-file function is an interactive function, and bound to C-c C-f. Inside the function, the external command gem is called through shell-command-to-string, but the feature-name parameters are not escaped. Thus, malicious Ruby source files may cause commands to be executed. | 7.3 | More Details |
| CVE-2023-0917 | A vulnerability, which was classified as critical, was found in SourceCodester Simple Customer Relationship Management System 1.0. This affects an unknown part of the file /php-scrm/login.php. The manipulation of the argument Password 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-221493 was assigned to this vulnerability. | 7.3 | More Details |
| CVE-2023-26266 | In AFL++ 4.05c, the CmpLog component uses the current working directory to resolve and execute unprefixed fuzzing targets, allowing code execution. | 7.3 | More Details |
| CVE-2022-26840 | Improper neutralization in the Intel(R) Quartus Prime Pro and Standard edition software may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.3 | More Details |
| CVE-2022-30704 | Improper initialization in the Intel(R) TXT SINIT ACM for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. | 7.2 | More Details |
| CVE-2022-38868 | SQL Injection vulnerability in Ehoney version 2.0.0 in models/protocol.go and models/images.go, allows attackers to execute arbitrary code. | 7.2 | More Details |
| CVE-2022-3901 | Prototype Pollution in Visioweb.js 1.10.6 allows attackers to execute XSS on the client system. | 7.2 | More Details |
| CVE-2022-33196 | Incorrect default permissions in some memory controller configurations for some Intel(R) Xeon(R) Processors when using Intel(R) Software Guard Extensions which may allow a privileged user to potentially enable escalation of privilege via local access. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-40677 | A improper neutralization of argument delimiters in a command ('argument injection') in Fortinet FortiNAC versions 9.4.0, 9.2.0 through 9.2.5, 9.1.0 through 9.1.7, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7 allows attacker to execute unauthorized code or commands via specially crafted input parameters. | 7.2 | More Details |
| CVE-2023-23007 | An issue was discovered in ESPCMS P8.21120101 after logging in to the background, there is a SQL injection vulnerability in the function node where members are added. | 7.2 | More Details |
| CVE-2022-27489 | A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiExtender 7.0.0 through 7.0.3, 5.3.2, 4.2.4 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests. | 7.2 | More Details |
| CVE-2022-38111 | SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. | 7.2 | More Details |
| CVE-2022-47503 | SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. | 7.2 | More Details |
| CVE-2022-47504 | SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. | 7.2 | More Details |
| CVE-2022-47507 | SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands. | 7.2 | More Details |
| CVE-2023-23836 | SolarWinds Platform version 2022.4.1 was found to be susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to the SolarWinds Web Console to execute arbitrary commands. | 7.2 | More Details |
| CVE-2023-0862 | The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. | 7.2 | More Details |
| CVE-2023-0861 | NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0895 | The WP Coder – add custom html, css and js code plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in versions up to, and including, 2.5.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrative privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | 7.2 | More Details |
| CVE-2022-33190 | Improper input validation in the Intel(R) SUR software before version 2.4.8902 may allow an authenticated user to potentially enable escalation of privilege via local access. | 7.1 | More Details |
| CVE-2021-32847 | HyperKit is a toolkit for embedding hypervisor capabilities in an application. In versions 0.20210107 and prior, a malicious guest can trigger a vulnerability in the host by abusing the disk driver that may lead to the disclosure of the host memory into the virtualized guest. This issue is fixed in commit cf60095a4d8c3cb2e182a14415467afd356e982f. | 7.1 | More Details |
| CVE-2023-22638 | Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. | 7.1 | More Details |
| CVE-2022-45153 | An Incorrect Default Permissions vulnerability in saphanabootstrap-formula of SUSE Linux Enterprise Module for SAP Applications 15-SP1, SUSE Linux Enterprise Server for SAP 12-SP5; openSUSE Leap 15.4 allows local attackers to escalate to root by manipulating the sudo configuration that is created. This issue affects: SUSE Linux Enterprise Module for SAP Applications 15-SP1 saphanabootstrap-formula versions prior to 0.13.1+git.1667812208.4db963e. SUSE Linux Enterprise Server for SAP 12-SP5 saphanabootstrap-formula versions prior to 0.13.1+git.1667812208.4db963e. openSUSE Leap 15.4 saphanabootstrap-formula versions prior to 0.13.1+git.1667812208.4db963e. | 7.0 | More Details |
| CVE-2020-19824 | An issue in MPV v.0.29.1 fixed in v0.30 allows attackers to execute arbitrary code and crash program via the ao_c parameter. | 7.0 | More Details |
| CVE-2022-32473 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the HddPassword shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-32470 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the FwBlockServiceSmm shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |
| CVE-2022-32955 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the NvmExpressDxe buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated by using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the link data to SMRAM before checking it and verifying that all pointers are within the buffer. | 7.0 | More Details |
| CVE-2023-0887 | A vulnerability was found in phjounin TFTPD64-SE 4.64 and classified as critical. This issue affects some unknown processing of the file tftpd64_svc.exe. The manipulation leads to unquoted search path. An attack has to be approached locally. The complexity of an attack is rather high. The exploitation is known to be difficult. The associated identifier of this vulnerability is VDB-221351. | 7.0 | More Details |
| CVE-2022-32954 | An issue was discovered in Insyde InsydeH2O with kernel 5.1 through 5.5. DMA attacks on the SdMmcDevice buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated by using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the link data to SMRAM before checking it and verifying that all pointers are within the buffer. | 7.0 | More Details |
| CVE-2022-32474 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the StorageSecurityCommandDxe shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |
| CVE-2022-32478 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the IdeBusDxe shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-32471 | An issue was discovered in IhisiSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. The IhisiDxe driver uses the command buffer to pass input and output data. By modifying the command buffer contents with DMA after the input parameters have been checked but before they are used, the IHISI SMM code may be convinced to modify SMRAM or OS, leading to possible data corruption or escalation of privileges. | 7.0 | More Details |
| CVE-2022-32953 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the SdHostDriver buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated by using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the link data to SMRAM before checking it and verifying that all pointers are within the buffer. | 7.0 | More Details |
| CVE-2022-32477 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the FvbServicesRuntimeDxe shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |
| CVE-2022-32475 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the VariableRuntimeDxe shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This issue was fixed in the kernel, which also protected chipset and OEM chipset code. | 7.0 | More Details |
| CVE-2022-32469 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the PnpSmm shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |
| CVE-2022-32476 | An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the AhciBusDxe shared buffer used by SMM and non-SMM code could cause TOCTOU race-condition issues that could lead to corruption of SMRAM and escalation of privileges. This attack can be mitigated using IOMMU protection for the ACPI runtime memory used for the command buffer. This attack can be mitigated by copying the firmware block services data to SMRAM before checking it. | 7.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48321 | Limited Server-Side Request Forgery (SSRF) in agent-receiver in Tribe29's Checkmk <= 2.1.0p11 allows an attacker to communicate with local network restricted endpoints by use of the host registration API. | 6.8 | More Details |
| CVE-2022-47909 | Livestatus Query Language (LQL) injection in the AuthUser HTTP query header of Tribe29's Checkmk <= 2.1.0p11, Checkmk <= 2.0.0p28, and all versions of Checkmk 1.6.0 (EOL) allows an attacker to perform direct queries to the application's core from localhost. | 6.8 | More Details |
| CVE-2023-23779 | Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. | 6.8 | More Details |
| CVE-2022-37329 | Uncontrolled search path in some Intel(R) Quartus(R) Prime Pro and Standard Edition software may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-41314 | Uncontrolled search path in some Intel(R) Network Adapter installer software may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-37340 | Uncontrolled search path in some Intel(R) QAT drivers for Windows before version 1.6 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-34854 | Improper access control in the Intel(R) SUR software before version 2.4.8902 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26425 | Uncontrolled search path element in the Intel(R) oneAPI Collective Communications Library (oneCCL) before version 2021.6 for Intel(R) oneAPI Base Toolkit may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26032 | Uncontrolled search path element in the Intel(R) Distribution for Python programming language before version 2022.1 for Intel(R) oneAPI Toolkits may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-34157 | Improper access control in the Intel(R) FPGA SDK for OpenCL(TM) with Intel(R) Quartus(R) Prime Pro Edition software before version 22.1 may allow authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-25905 | Uncontrolled search path element in the Intel(R) oneAPI Data Analytics Library (oneDAL) before version 2021.5 for Intel(R) oneAPI Base Toolkit may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-32570 | Improper authentication in the Intel(R) Quartus Prime Pro and Standard edition software may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26052 | Uncontrolled search path element in the Intel(R) MPI Library before version 2021.6 for Intel(R) oneAPI HPC Toolkit may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26062 | Uncontrolled search path element in the Intel(R) Trace Analyzer and Collector before version 2021.6 for Intel(R) oneAPI HPC Toolkit may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2023-23783 | A use of externally-controlled format string in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. | 6.7 | More Details |
| CVE-2022-36398 | Uncontrolled search path in the Intel(R) Battery Life Diagnostic Tool software before version 2.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26076 | Uncontrolled search path element in the Intel(R) oneAPI Deep Neural Network (oneDNN) before version 2022.1 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26512 | Uncontrolled search path element in the Intel(R) FPGA Add-on for Intel(R) oneAPI Base Toolkit before version 2022.2 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26421 | Uncontrolled search path element in the Intel(R) oneAPI DPC++/C++ Compiler Runtime before version 2022.0 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2022-26345 | Uncontrolled search path element in the Intel(R) oneAPI Toolkit OpenMP before version 2022.1 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.7 | More Details |
| CVE-2023-26234 | JD-GUI 1.6.6 allows deserialization via UIMainWindowPreferencesProvider.singleInstance. | 6.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-33871 | A stack-based buffer overflow vulnerability [CWE-121] in FortiWeb version 7.0.1 and earlier, 6.4 all versions, version 6.3.19 and earlier may allow a privileged attacker to execute arbitrary code or commands via specifically crafted CLI `execute backup-local rename` and `execute backup-local show` operations. | 6.6 | More Details |
| CVE-2022-48282 | Under very specific circumstances (see Required configuration section below), a privileged user is able to cause arbitrary code to be executed which may cause further disruption to services. This is specific to applications written in C#. This affects all MongoDB .NET/C# Driver versions prior to and including v2.18.0 Following configuration must be true for the vulnerability to be applicable: * Application must written in C# taking arbitrary data from users and serializing data using _t without any validation AND * Application must be running on a Windows host using the full .NET Framework, not .NET Core AND * Application must have domain model class with a property/field explicitly of type System.Object or a collection of type System.Object (against MongoDB best practice) AND * Malicious attacker must have unrestricted insert access to target database to add a _t discriminator."Following configuration must be true for the vulnerability to be applicable | 6.6 | More Details |
| CVE-2022-30306 | A stack-based buffer overflow vulnerability [CWE-121] in the CA sign functionality of FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted password. | 6.6 | More Details |
| CVE-2023-25768 | A missing permission check in Jenkins Azure Credentials Plugin 253.v887e0f9e898b and earlier allows attackers with Overall/Read permission to connect to an attacker-specified web server. | 6.5 | More Details |
| CVE-2022-45437 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Artica PFMS Pandora FMS v765 on all allows Cross-Site Scripting (XSS). A user with edition privileges can create a Payload in the reporting dashboard module. An admin user can observe the Payload without interaction and attacker can get information. | 6.5 | More Details |
| CVE-2022-40675 | Some cryptographic issues in Fortinet FortiNAC versions 9.4.0 through 9.4.1, 9.2.0 through 9.2.7, 9.1.0 through 9.1.8, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 8.6.0 through 8.6.5, 8.5.0 through 8.5.4, 8.3.7 may allow an attacker to decrypt and forge protocol communication messages. | 6.5 | More Details |
| CVE-2021-33396 | Cross Site Request Forgery (CSRF) vulnerability in baijiacms 4.1.4, allows attackers to change the password or other information of an arbitrary account via index.php. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-36775 | IBM Security Verify Access 10.0.0.0, 10.0.1.0, 10.0.2.0, 10.0.3.0, and10.0.4.0 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 233576. | 6.5 | More Details |
| CVE-2023-23466 | Media CP Media Control Panel latest version. Insufficiently protected credential change. | 6.5 | More Details |
| CVE-2022-29494 | Improper input validation in firmware for OpenBMC in some Intel(R) platforms before versions egs-0.91-179 and bhs-04-45 may allow an authenticated user to potentially enable denial of service via network access. | 6.5 | More Details |
| CVE-2021-33104 | Improper access control in the Intel(R) OFU software before version 14.1.28 may allow an authenticated user to potentially enable denial of service via local access. | 6.5 | More Details |
| CVE-2023-22380 | A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.6. This vulnerability was reported via the GitHub Bug Bounty program. | 6.5 | More Details |
| CVE-2022-30300 | A relative path traversal vulnerability [CWE-23] in FortiWeb 7.0.0 through 7.0.1, 6.3.6 through 6.3.18, 6.4 all versions may allow an authenticated attacker to obtain unauthorized access to files and data via specifically crafted HTTP GET requests. | 6.5 | More Details |
| CVE-2023-23009 | Libreswan 4.9 allows remote attackers to cause a denial of service (assert failure and daemon restart) via crafted TS payload with an incorrect selector length. | 6.5 | More Details |
| CVE-2023-22805 | LS ELECTRIC XBC-DN32U with operating system version 01.80 has improper access control to its read prohibition feature. This could allow a remote attacker to remotely set the feature to lock users out of reading data from the device. | 6.5 | More Details |
| CVE-2023-23458 | Sunell DVR, latest version, CWE-200: Exposure of Sensitive Information to an Unauthorized Actor through an unspecified request. | 6.5 | More Details |
| CVE-2023-26267 | php-saml-sp before 1.1.1 and 2.x before 2.1.1 allows reading arbitrary files as the webserver user because resolving XML external entities was silently enabled via \LIBXML_DTDLOAD \| \LIBXML_DTDATTR. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0821 | HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in 1.2.16, 1.3.9, and 1.4.4. | 6.5 | More Details |
| CVE-2022-48319 | Sensitive host secret disclosed in cmk-update-agent.log file in Tribe29's Checkmk <= 2.1.0p13, Checkmk <= 2.0.0p29, and all versions of Checkmk 1.6.0 (EOL) allows an attacker to gain access to the host secret through the unprotected agent updater log file. | 6.5 | More Details |
| CVE-2023-23936 | Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. | 6.5 | More Details |
| CVE-2023-25812 | Minio is a Multi-Cloud Object Storage framework. Affected versions do not correctly honor a `Deny` policy on ByPassGoverance. Ideally, minio should return "Access Denied" to all users attempting to DELETE a versionId with the special header `X-Amz-Bypass-Governance-Retention: true`. However, this was not honored instead the request will be honored and an object under governance would be incorrectly deleted. All users are advised to upgrade. There are no known workarounds for this issue. | 6.5 | More Details |
| CVE-2023-0936 | A vulnerability was found in TP-Link Archer C50 V2_160801. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation leads to denial of service. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221552. | 6.5 | More Details |
| CVE-2022-47373 | Reflected Cross Site Scripting in Search Functionality of Module Library in Pandora FMS Console v766 and lower. This vulnerability arises on the forget password functionality in which parameter username does not proper input validation/sanitization thus results in executing malicious JavaScript payload. | 6.4 | More Details |
| CVE-2023-23781 | A stack-based buffer overflow vulnerability [CWE-121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server configuration may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted XML files. | 6.4 | More Details |
| CVE-2023-0879 | Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpayserver prior to 1.7.12. | 6.3 | More Details |
| CVE-2022-40232 | IBM Sterling B2B Integrator Standard Edition 6.1.0.0 through 6.1.1.1, and 6.1.2.0 could allow an authenticated user to perform actions they should not have access to due to improper permission controls. IBM X-Force ID: 235597. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0904 | A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file task-details.php. The manipulation of the argument task_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221453 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-0883 | A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file /php-opos/index.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-221350 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-0938 | A vulnerability classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file music_list.php of the component GET Request Handler. The manipulation of the argument cid 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-221553 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2022-48307 | It was discovered that the Magritte-ftp was not verifying hostnames in TLS certificates due to a misuse of the javax.net.ssl.SSLSocketFactory API. A malicious attacker in a privileged network position could abuse this to perform a man-in-the-middle attack. A successful man-in-the-middle attack would allow them to intercept, read, or modify network communications to and from the affected service. In the case of a successful man in the middle attack on magritte-ftp, an attacker would be able to read and modify network traffic such as authentication tokens or raw data entering a Palantir Foundry stack. | 6.3 | More Details |
| CVE-2023-0935 | A vulnerability was found in DolphinPHP up to 1.5.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file common.php of the component Incomplete Fix CVE-2021-46097. The manipulation of the argument id leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221551. | 6.3 | More Details |
| CVE-2022-48308 | It was discovered that the sls-logging was not verifying hostnames in TLS certificates due to a misuse of the javax.net.ssl.SSLSocketFactory API. A malicious attacker in a privileged network position could abuse this to perform a man-in-the-middle attack. A successful man-in-the-middle attack would allow them to intercept, read, or modify network communications to and from the affected service. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0910 | A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_prod.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-221476. | 6.3 | More Details |
| CVE-2023-25810 | Uptime Kuma is a self-hosted monitoring tool. In versions prior to 1.20.0 the Uptime Kuma status page allows a persistent XSS attack. Users are advised to upgrade. There are no known workarounds for this vulnerability. | 6.3 | More Details |
| CVE-2023-0915 | A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. Affected is an unknown function of the file /adms/admin/?page=user/manage_user. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221490 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2022-27808 | Insufficient control flow management in some Intel(R) Ethernet Controller Administrative Tools drivers for Windows before version 1.5.0.2 may allow an authenticated user to potentially enable escalation of privilege via local access. | 6.3 | More Details |
| CVE-2013-10019 | A vulnerability was found in OCLC-Research OAICat 1.5.61. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The attack may be initiated remotely. Upgrading to version 1.5.62 is able to address this issue. The identifier of the patch is 6cc65501869fa663bcd24a70b63f41f5cfe6b3e1. It is recommended to upgrade the affected component. The identifier VDB-221489 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2012-10008 | A vulnerability, which was classified as critical, has been found in uakfdotb oneapp. This issue affects some unknown processing. The manipulation leads to sql injection. The attack may be initiated remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 5413ac804f1b09f9decc46a6c37b08352c49669c. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-221483. | 6.3 | More Details |
| CVE-2023-0841 | A vulnerability, which was classified as critical, has been found in GPAC 2.3-DEV-rev40-g3602a5ded. This issue affects the function mp3_dmx_process of the file filters/reframe_mp3.c. The manipulation leads to heap-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221087. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25811 | Uptime Kuma is a self-hosted monitoring tool. In versions prior to 1.20.0 the Uptime Kuma `name` parameter allows a persistent XSS attack. Users are advised to upgrade. There are no known workarounds for this vulnerability. | 6.3 | More Details |
| CVE-2015-10083 | A vulnerability has been found in harrystech Dynosaur-Rails and classified as critical. Affected by this vulnerability is the function basic_auth of the file app/controllers/application_controller.rb. The manipulation leads to improper authentication. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 04b223813f0e336aab50bff140d0f5889c31dbec. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-221503. | 6.3 | More Details |
| CVE-2023-0946 | A vulnerability has been found in SourceCodester Best POS Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file billing/index.php?id=9. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-221593 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-0918 | A vulnerability has been found in codeprojects Pharmacy Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file add.php of the component Avatar Image Handler. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221494 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2017-20179 | A vulnerability was found in InSTEDD Pollit 2.3.1. It has been rated as critical. This issue affects the function TourController of the file app/controllers/tour_controller.rb. The manipulation leads to an unknown weakness. The attack may be initiated remotely. Upgrading to version 2.3.2 is able to address this issue. The patch is named 6ef04f8b5972d5f16f8b86f8b53f62fac68d5498. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-221507. | 6.3 | More Details |
| CVE-2023-0916 | A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /adms/classes/Users.php. The manipulation leads to improper access controls. 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-221491. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-27890 | It was discovered that the sls-logging was not verifying hostnames in TLS certificates due to a misuse of the javax.net.ssl.SSLSocketFactory API. A malicious attacker in a privileged network position could abuse this to perform a man-in-the-middle attack. A successful man-in-the-middle attack would allow them to intercept, read, or modify network communications to and from the affected service. In the case of AtlasDB, the vulnerability was mitigated by other network controls such as two-way TLS when deployed as part of a Palantir platform. Palantir still recommends upgrading to a non-vulnerable version out of an abundance of caution. | 6.3 | More Details |
| CVE-2023-23558 | In Eternal Terminal 6.2.1, TelemetryService uses fixed paths in /tmp. For example, a local attacker can create /tmp/.sentry-native-etserver with mode 0777 before the etserver process is started. The attacker can choose to read sensitive information from that file, or modify the information in that file. | 6.3 | More Details |
| CVE-2023-24964 | IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information from a log files. IBM X-Force ID: 246463. | 6.2 | More Details |
| CVE-2023-25153 | containerd is an open source container runtime. Before versions 1.6.18 and 1.5.18, when importing an OCI image, there was no limit on the number of bytes read for certain files. A maliciously crafted image with a large file where a limit was not applied could cause a denial of service. This bug has been fixed in containerd 1.6.18 and 1.5.18. Users should update to these versions to resolve the issue. As a workaround, ensure that only trusted images are used and that only trusted users have permissions to import images. | 6.2 | More Details |
| CVE-2021-32844 | HyperKit is a toolkit for embedding hypervisor capabilities in an application. In versions 0.20210107 and prior of HyperKit, ` vi_pci_write` has is a call to `vc_cfgwrite` that does not check for null which when called makes the host crash. This issue may lead to a guest crashing the host causing a denial of service. This issue is fixed in commit 451558fe8aaa8b24e02e34106e3bb9fe41d7ad13. | 6.2 | More Details |
| CVE-2022-43930 | IBM Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 is vulnerable to an Information Disclosure as sensitive information may be included in a log file. IBM X-Force ID: 241677. | 6.2 | More Details |
| CVE-2021-32843 | HyperKit is a toolkit for embedding hypervisor capabilities in an application. In versions 0.20210107 and prior of HyperKit, `virtio.c` has is a call to `vc_cfgread` that does not check for null which when called makes the host crash. This issue may lead to a guest crashing the host causing a denial of service. This issue is fixed in commit df0e46c7dbfd81a957d85e449ba41b52f6f7beb4. | 6.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32850 | jQuery MiniColors is a color picker built on jQuery. Prior to version 2.3.6, jQuery MiniColors is prone to cross-site scripting when handling untrusted color names. This issue is patched in version 2.3.6. | 6.1 | More Details |
| CVE-2022-4897 | The BackupBuddy WordPress plugin before 8.8.3 does not sanitise and escape some parameters before outputting them back in various places, leading to Reflected Cross-Site Scripting | 6.1 | More Details |
| CVE-2023-0428 | The Watu Quiz WordPress plugin before 3.3.8.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin. | 6.1 | More Details |
| CVE-2022-48115 | The dropdown menu in jspreadsheet before v4.6.0 was discovered to be vulnerable to cross-site scripting (XSS). | 6.1 | More Details |
| CVE-2021-23980 | A mutation XSS affects users calling bleach.clean with all of: svg or math in the allowed tags p or br in allowed tags style, title, noscript, script, textarea, noframes, iframe, or xmp in allowed tags the keyword argument strip_comments=False Note: none of the above tags are in the default allowed tags and strip_comments defaults to True. | 6.1 | More Details |
| CVE-2021-32855 | Vditor is a browser-side Markdown editor. Versions prior to 3.8.7 are vulnerable to copy-paste cross-site scripting (XSS). For this particular type of XSS, the victim needs to be fooled into copying a malicious payload into the text editor. Version 3.8.7 contains a patch for this issue. | 6.1 | More Details |
| CVE-2021-32854 | textAngular is a text editor for Angular.js. Version 1.5.16 and prior are vulnerable to copy-paste cross-site scripting (XSS). For this particular type of XSS, the victim needs to be fooled into copying a malicious payload into the text editor. There are no known patches. | 6.1 | More Details |
| CVE-2022-33972 | Incorrect calculation in microcode keying mechanism for some 3rd Generation Intel(R) Xeon(R) Scalable Processors may allow a privileged user to potentially enable information disclosure via local access. | 6.1 | More Details |
| CVE-2021-32856 | Microweber is a drag and drop website builder and content management system. Versions 1.2.12 and prior are vulnerable to copy-paste cross-site scripting (XSS). For this particular type of XSS, the victim needs to be fooled into copying a malicious payload into the text editor. A fix was attempted in versions 1.2.9 and 1.2.12, but it is incomplete. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48327 | Multiple Cross Site Scripting (XSS) vulnerabilities in Mapos 4.39.0 allow attackers to execute arbitrary code. Affects the following parameters: (1) dataInicial, (2) dataFinal, (3) tipocliente, (4) format, (5) precoInicial, (6) precoFinal, (7) estoqueInicial, (8) estoqueFinal, (9) de_id, (10) ate_id, (11) clientes_id, (12) origem, (13) cliente, (14) responsavel, (15) status, (16) tipo, (17) situacao in file application/controllers/Relatorios.php; (18) preco, (19) nome, (20) descricao, (21) idServicos, (22) id in file application/controllers/Servicos.php; (23) senha, (24) permissoes_id, (25) idUsuarios, (26) situacao, (27) nome, (28) rg, (29) cpf, (30) cep, (31) rua, (32) numero, (33) bairro, (34) cidade, (35) estado, (36) email, (37) telefone, (38) celular in file application/controllers/Usuarios.php; (39) dataVenda, (40) observacoes, (41) observacoes_cliente, (42) clientes_id, (43) usuarios_id, (44) idVendas, (45) id, (46) idVendasProduto, (47) preco, (48) quantidade, (49) idProduto, (50) produto, (51) desconto, (52) tipoDesconto, (53) resultado, (54) vendas_id, (55) vencimento, (56) recebimento, (57) valor, (58) recebido, (59) formaPgto, (60) tipo in file application/controllers/Vendas.php; (61) situacao, (62) periodo, (63) vencimento_de, (64) vencimento_ate, (65) tipo, (66) status, (67) cliente in file application/views/financeiro/lancamentos.php; (68) year in file application/views/mapos/painel.php; (69) pesquisa in file application/views/os/os.php; (70) etiquetaCode in file application/views/relatorios/imprimir/imprimirEtiquetas.php. | 6.1 | More Details |
| CVE-2021-32857 | Cockpit is a content management system that allows addition of content management functionality to any site. In versions 0.12.2 and prior, bad HTML sanitization in `htmleditor.js` may lead to cross-site scripting (XSS) issues. There are no known patches for this issue. | 6.1 | More Details |
| CVE-2023-23922 | The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. | 6.1 | More Details |
| CVE-2023-23921 | The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. | 6.1 | More Details |
| CVE-2023-0442 | The Loan Comparison WordPress plugin before 1.5.3 does not validate and escape some of its query parameters before outputting them back in a page/post via an embedded shortcode, which could allow an attacker to inject javascript into into the site via a crafted URL. | 6.1 | More Details |
| CVE-2022-0637 | open redirect in pollbot (pollbot.services.mozilla.com) in versions before 1.4.6 | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32858 | esdoc-publish-html-plugin is a plugin for the document maintenance software ESDoc. TheHTML sanitizer in esdoc-publish-html-plugin 1.1.2 and prior can be bypassed which may lead to cross-site scripting (XSS) issues. There are no known patches for this issue. | 6.1 | More Details |
| CVE-2022-45436 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Artica PFMS Pandora FMS v765 on all platforms, allows Cross-Site Scripting (XSS). As a manager privilege user , create a network map containing name as xss payload. Once created, admin user must click on the edit network maps and XSS payload will be executed, which could be used for stealing admin users cookie value. | 6.1 | More Details |
| CVE-2022-45543 | Cross site scripting (XSS) vulnerability in DiscuzX 3.4 allows attackers to execute arbitrary code via the datetline, title, tpp, or username parameters via the audit search. | 6.1 | More Details |
| CVE-2023-0942 | The Japanized For WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘tab’ parameter in versions up to, and including, 2.5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. | 6.1 | More Details |
| CVE-2021-32851 | Mind-elixir is a free, open source mind map core. Prior to version 0.18.1, mind-elixir is prone to cross-site scripting when handling untrusted menus. This issue is patched in version 0.18.1 | 6.1 | More Details |
| CVE-2023-22984 | A Vulnerability was discovered in Axis 207W network camera. There is a reflected XSS vulnerability in the web administration portal, which allows an attacker to execute arbitrary JavaScript via URL. | 6.1 | More Details |
| CVE-2022-38376 | Multiple improper neutralization of input during web page generation ('Cross-site Scripting') vulnerabilities [CWE-79] in Fortinet FortiNAC portal UI before 9.4.1 allows an attacker to perform an XSS attack via crafted HTTP requests. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48324 | Multiple Cross Site Scripting (XSS) vulnerabilities in Mapos 4.39.0 allow attackers to execute arbitrary code. Affects the following parameters: (1) pesquisa, (2) data, (3) data2, (4) nome, (5) descricao, (6) idDocumentos, (7) id in file application/controllers/Arquivos.php; (8) senha, (9) nomeCliente, (10) contato, (11) documento, (12) telefone, (13) celular, (14) email, (15) rua, (16) numero, (17) complemento, (18) bairro, (19) cidade, (20) estado, (21) cep, (22) idClientes, (23) id in file application/controllers/Clientes.php; (24) id, (25) tipo, (26) forma_pagamento, (27) gateway_de_pagamento, (28) excluir_id, (29) confirma_id, (30) cancela_id in file application/controllers/Cobrancas.php; (31) vencimento_de, (32) vencimento_ate, (33) cliente, (34) tipo, (35) status, (36) valor_desconto, (37) desconto, (38) periodo, (39) per_page, (40) urlAtual, (41) vencimento, (42) recebimento, (43) valor, (44) recebido, (45) formaPgto, (46) desconto_parc, (47) entrada, (48) qtdparcelas_parc, (49) valor_parc, (50) dia_pgto, (51) dia_base_pgto, (52) comissao, (53) descricao_parc, (54) cliente_parc, (55) observacoes_parc, (56) formaPgto_parc, (57) tipo_parc, (58) pagamento, (59) pago, (60) valor_desconto_editar, (61) descricao, (62) fornecedor, (63) observacoes, (64) id in file application/controllers/Financeiro.php; (65) refGarantia, (66) textoGarantia, (67) idGarantias in file application/controllers/Garantias.php; (68) email, (69) senha in file application/controllers/Login.php. | 6.1 | More Details |
| CVE-2023-0878 | Cross-site Scripting (XSS) - Generic in GitHub repository nuxt/framework prior to 3.2.1. | 6.1 | More Details |
| CVE-2023-24369 | A cross-site scripting (XSS) vulnerability in UJCMS v4.1.3 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the URL parameter under the Add New Articles function. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2022-48325 | Multiple Cross Site Scripting (XSS) vulnerabilities in Mapos 4.39.0 allow attackers to execute arbitrary code. Affects the following parameters: (1) year, (2) oldSenha, (3) novaSenha, (4) termo, (5) nome, (6) cnpj, (7) ie, (8) cep, (9) logradouro, (10) numero, (11) bairro, (12) cidade, (13) uf, (14) telefone, (15) email, (16) id, (17) app_name, (18) per_page, (19) app_theme, (20) os_notification, (21) email_automatico, (22) control_estoque, (23) notifica_whats, (24) control_baixa, (25) control_editos, (26) control_edit_vendas, (27) control_datatable, (28) pix_key, (29) os_status_list, (30) control_2vias, (31) status, (32) start, (33) end in file application/controllers/Mapos.php; (34) token, (35) senha, (36) email, (37) nomeCliente, (38) documento, (39) telefone, (40) celular, (41) rua, (42) numero, (43) complemento, (44) bairro, (45) cidade, (46) estado, (47) cep, (48) idClientes, (49) descricaoProduto, (50) defeito in file application/controllers/Mine.php; (51) pesquisa, (52) status, (53) data, (54) data2, (55) dataInicial, (56) dataFinal, (57) termoGarantia, (58) garantias_id, (59) clientes_id, (60) usuarios_id, (61) idOs, (62) garantia, (63) descricaoProduto, (64) defeito, (65) observacoes, (66) laudoTecnico, (67) id, (68) preco, (69) quantidade, (70) idProduto, (71) idOsProduto, (72) produto, (73) idServico, (74) idOsServico, (75) desconto, (76) tipoDesconto, (77) resultado, (78) vencimento, (79) recebimento, (80) os_id, (81) valor, (82) recebido, (83) formaPgto, (84) tipo, (85) anotacao, (86) idAnotacao in file application/controllers/Os.php. | 6.1 | More Details |
| CVE-2021-32859 | The Baremetrics date range picker is a solution for selecting both date ranges and single dates from a single calender view. Versions 1.0.14 and prior are prone to cross-site scripting (XSS) when handling untrusted `placeholder` entries. An attacker who is able to influence the field `placeholder` when creating a `Calendar` instance is able to supply arbitrary `html` or `javascript` that will be rendered in the context of a user leading to XSS. There are no known patches for this issue. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-48326 | Multiple Cross Site Scripting (XSS) vulnerabilities in Mapos 4.39.0 allow attackers to execute arbitrary code. Affects the following parameters: (1) nome, (2) aCliente, (3) eCliente, (4) dCliente, (5) vCliente, (6) aProduto, (7) eProduto, (8) dProduto, (9) vProduto, (10) aServico, (11) eServico, (12) dServico, (13) vServico, (14) aOs, (15) eOs, (16) dOs, (17) vOs, (18) aVenda, (19) eVenda, (20) dVenda, (21) vVenda, (22) aGarantia, (23) eGarantia, (24) dGarantia, (25) vGarantia, (26) aArquivo, (27) eArquivo, (28) dArquivo, (29) vArquivo, (30) aPagamento, (31) ePagamento, (32) dPagamento, (33) vPagamento, (34) aLancamento, (35) eLancamento, (36) dLancamento, (37) vLancamento, (38) cUsuario, (39) cEmitente, (40) cPermissao, (41) cBackup, (42) cAuditoria, (43) cEmail, (44) cSistema, (45) rCliente, (46) rProduto, (47) rServico, (48) rOs, (49) rVenda, (50) rFinanceiro, (51) aCobranca, (52) eCobranca, (53) dCobranca, (54) vCobranca, (55) situacao, (56) idPermissao, (57) id in file application/controllers/Permissoes.php; (58) precoCompra, (59) precoVenda, (60) descricao, (61) unidade, (62) estoque, (63) estoqueMinimo, (64) idProdutos, (65) id, (66) estoqueAtual in file application/controllers/Produtos.php. | 6.1 | More Details |
| CVE-2021-32860 | iziModal is a modal plugin with jQuery. Versions prior to 1.6.1 are vulnerable to cross-site scripting (XSS) when handling untrusted modal titles. An attacker who is able to influence the field `title` when creating a `iziModal` instance is able to supply arbitrary `html` or `javascript` code that will be rendered in the context of a user, potentially leading to `XSS`. Version 1.6.1 contains a patch for this issue | 6.1 | More Details |
| CVE-2021-32853 | Erxes, an experience operating system (XOS) with a set of plugins, is vulnerable to cross-site scripting in versions 0.22.3 and prior. This results in client-side code execution. The victim must follow a malicious link or be redirected there from malicious web site. There are no known patches. | 6.1 | More Details |
| CVE-2023-26235 | JD-GUI 1.6.6 allows XSS via util/net/InterProcessCommunicationUtil.java. | 6.1 | More Details |
| CVE-2019-17003 | Scanning a QR code that contained a javascript: URL would have resulted in the Javascript being executed. | 6.1 | More Details |
| CVE-2022-36794 | Improper condition check in some Intel(R) SPS firmware before version SPS_E3_06.00.03.300.0 may allow a privileged user to potentially enable denial of service via local access. | 6.0 | More Details |
| CVE-2022-36382 | Out-of-bounds write in firmware for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 1.7.0.8 and some Intel(R) Ethernet 700 Series Controllers and Adapters before version 9.101 may allow a privileged user to potentially enable denial of service via local access. | 6.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-38090 | Improper isolation of shared resources in some Intel(R) Processors when using Intel(R) Software Guard Extensions may allow a privileged user to potentially enable information disclosure via local access. | 6.0 | More Details |
| CVE-2022-30339 | Out-of-bounds read in firmware for the Intel(R) Integrated Sensor Solution before versions 5.4.2.4579v3, 5.4.1.4479 and 5.0.0.4143 may allow a privileged user to potentially enable denial of service via local access. | 6.0 | More Details |
| CVE-2023-23926 | APOC (Awesome Procedures on Cypher) is an add-on library for Neo4j. An XML External Entity (XXE) vulnerability found in the apoc.import.graphml procedure of APOC core plugin prior to version 5.5.0 and 4.4.0.14 (4.4 branch) in Neo4j graph database. XML External Entity (XXE) injection occurs when the XML parser allows external entities to be resolved. The XML parser used by the apoc.import.graphml procedure was not configured in a secure way and therefore allowed this. External entities can be used to read local files, send HTTP requests, and perform denial-of-service attacks on the application. Abusing the XXE vulnerability enabled assessors to read local files remotely. Although with the level of privileges assessors had this was limited to one-line files. With the ability to write to the database, any file could have been read. Additionally, assessors noted, with local testing, the server could be crashed by passing in improperly formatted XML. The minimum version containing a patch for this vulnerability is 5.5.0. Those who cannot upgrade the library can control the allowlist of the procedures that can be used in your system. | 5.9 | More Details |
| | A vulnerability exists in the IEC 61850 communication stack that affects multiple Hitachi Energy products. An attacker could exploit the vulnerability by using a specially crafted message sequence, to force the IEC 61850 MMS-server communication stack, to stop accepting new MMS-client connections. Already existing/established client-server connections are not affected. List of affected CPEs: * cpe:2.3:o:hitachienergy:fox61x_tego1:r15b08:*:*:*:*:*:*:* * cpe:2.3:o:hitachienergy:fox61x_tego1:r2a16_3:*:*:*:*:*:*:* * cpe:2.3:o:hitachienergy:fox61x_tego1:r2a16:*:*:*:*:*:*:* * cpe:2.3:o:hitachienergy:fox61x_tego1:r1e01:*:*:*:*:*:*:* * cpe:2.3:o:hitachienergy:fox61x_tego1:r1d02:*:*:*:*:*:*:* * cpe:2.3:o:hitachienergy:fox61x_tego1:r1c07:*:*:*:*:*:*:* * cpe:2.3:o:hitachienergy:fox61x_tego1:r1b02:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:gms600:1.3.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.1.*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.5.*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.6.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.6.0.1:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.7.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.7.2:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:1.8.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:2.0.*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:2.1.0.4:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:itt600_sa_explorer:2.1.0.5:*:*:*:*:*:*:* * | | |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-3353 | cpe:2.3:a:hitachienergy:microscada_x_sys600:10:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.*:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.2:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.2.1:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.3:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.3.1:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.4:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:microscada_x_sys600:10.4.1:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:mms:2.2.3:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:pwc600:1.0:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:pwc600:1.1:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:pwc600:1.2:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:reb500:7:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:reb500:8:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion670:1.2.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion670:2.0.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion650:1.1.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion650:1.3.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion650:2.1.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion670:2.1.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relionSAM600-IO:2.2.1:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relionSAM600-IO:2.2.5:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion670:2.2.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:relion650:2.2.*:*:*:*:*:*:*:* *<br>cpe:2.3:o:hitachienergy:rtu500cmu:12.*.*:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:rtu500cmu:13.*.*:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:txpert_hub_coretec_4:2.*:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:txpert_hub_coretec_4:3.0:*:*:*:*:*:*:* *<br>cpe:2.3:a:hitachienergy:txpert_hub_coretec_5:3.0:*:*:*:*:*:*:* | 5.9 | More Details |
| CVE-2022-30692 | Improper conditions check in the Intel(R) SUR software before version 2.4.8902 may allow an unauthenticated user to potentially enable denial of service via network access. | 5.9 | More Details |
| CVE-2020-12413 | The Raccoon attack is a timing attack on DHE ciphersuites inherit in the TLS specification. To mitigate this vulnerability, Firefox disabled support for DHE ciphersuites. | 5.9 | More Details |
| CVE-2022-34351 | IBM QRadar SIEM 7.4 and 7.5 is vulnerable to information exposure allowing a non-tenant user with a specific domain security profile assigned to see some data from other domains. IBM X-Force ID: 230402. | 5.9 | More Details |
| CVE-2023-23695 | Dell Secure Connect Gateway (SCG) version 5.14.00.12 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information. | 5.9 | More Details |
| CVE-2022-43927 | IBM Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 is vulnerable to information Disclosure due to improper privilege management when a specially crafted table access is used. IBM X-Force ID: 241671. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-26115 | A use of password hash with insufficient computational effort vulnerability [CWE-916] in FortiSandbox before 4.2.0 may allow an attacker with access to the password database to efficiently mount bulk guessing attacks to recover the passwords. | 5.9 | More Details |
| CVE-2023-25569 | Apollo is a configuration management system. Prior to version 2.1.0, a low-privileged user can create a special web page. If an authenticated portal admin visits this page, the page can silently send a request to assign new roles for that user without any confirmation from the Portal admin. Cookie SameSite strategy was set to Lax in version 2.1.0. As a workaround, avoid visiting unknown source pages. | 5.7 | More Details |
| CVE-2022-48306 | Improper Validation of Certificate with Host Mismatch vulnerability in Gotham Chat IRC helper of Palantir Gotham allows A malicious attacker in a privileged network position could abuse this to perform a man-in-the-middle attack. A successful man-in-the-middle attack would allow them to intercept, read, or modify network communications to and from the affected service. This issue affects: Palantir Palantir Gotham Chat IRC helper versions prior to 30221005.210011.9242. | 5.7 | More Details |
| CVE-2022-27170 | Protection mechanism failure in the Intel(R) Media SDK software before version 22.2.2 may allow an authenticated user to potentially enable escalation of privilege via local access. | 5.7 | More Details |
| CVE-2023-23784 | A relative path traversal in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to information disclosure via specially crafted web requests. | 5.7 | More Details |
| CVE-2023-26020 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. | 5.7 | More Details |
| CVE-2022-34841 | Improper buffer restrictions in the Intel(R) Media SDK software before version 22.2.2 may allow an authenticated user to potentially enable escalation of privilege via local access. | 5.7 | More Details |
| CVE-2022-48317 | Expired sessions were not securely terminated in the RestAPI for Tribe29's Checkmk <= 2.1.0p10 and Checkmk <= 2.0.0p28 allowing an attacker to use expired session tokens when communicating with the RestAPI. | 5.6 | More Details |
| CVE-2021-26277 | The framework service handles pendingIntent incorrectly, allowing a malicious application with certain privileges to perform privileged actions. | 5.6 | More Details |
| CVE-2022-33946 | Improper authentication in the Intel(R) SUR software before version 2.4.8902 may allow an authenticated user to potentially enable escalation of privilege via local access. | 5.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0908 | A vulnerability, which was classified as problematic, was found in Xoslab Easy File Locker 2.2.0.184. This affects the function MessageNotifyCallback in the library xlkfs.sys. 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 VDB-221457 was assigned to this vulnerability. | 5.5 | More Details |
| CVE-2014-125087 | A vulnerability was found in java-xmlbuilder up to 1.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to xml external entity reference. Upgrading to version 1.2 is able to address this issue. The name of the patch is e6fddca201790abab4f2c274341c0bb8835c3e73. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-221480. | 5.5 | More Details |
| CVE-2022-45586 | Stack overflow vulnerability in function Dict::find in xpdf/Dict.cc in xpdf 4.04, allows local attackers to cause a denial of service. | 5.5 | More Details |
| CVE-2022-45587 | Stack overflow vulnerability in function gmalloc in goo/gmem.cc in xpdf 4.04, allows local attackers to cause a denial of service. | 5.5 | More Details |
| CVE-2023-22233 | After Affects versions 23.1 (and earlier), 22.6.3 (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 | More Details |
| CVE-2023-24484 | A malicious user can cause log files to be written to a directory that they do not have permission to write to. | 5.5 | More Details |
| CVE-2023-22231 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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 | More Details |
| CVE-2023-0482 | In RESTEasy the insecure File.createTempFile() is used in the DataSourceProvider, FileProvider and Mime4JWorkaround classes which creates temp files with insecure permissions that could be read by a local user. | 5.5 | More Details |
| CVE-2022-31476 | Improper access control in the Intel(R) SUR software before version 2.4.8902 may allow an authenticated user to potentially enable denial of service via local access. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2015-10084 | A vulnerability was found in irontec klear-library chloe and classified as critical. Affected by this issue is the function _prepareWhere of the file Controller/Rest/BaseController.php. The manipulation leads to sql injection. Upgrading to version marla is able to address this issue. The name of the patch is b25262de52fdaffde2a4434fc2a84408b304fbc5. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-221504. | 5.5 | More Details |
| CVE-2022-41614 | Insufficiently protected credentials in the Intel(R) ON Event Series Android application before version 2.0 may allow an authenticated user to potentially enable information disclosure via local access. | 5.5 | More Details |
| CVE-2015-10082 | A vulnerability classified as problematic has been found in UIKit0 libplist 1.12. This affects the function plist_from_xml of the file src/xplist.c of the component XML Handler. The manipulation leads to xml external entity reference. The patch is named c086cb139af7c82845f6d565e636073ff4b37440. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-221499. | 5.5 | More Details |
| CVE-2023-24785 | An issue in Giorgio Tani peazip v.9.0.0 allows attackers to cause a denial of service via the End of Archive tag function of the peazip/pea UNPEA feature. | 5.5 | More Details |
| CVE-2023-23586 | Due to a vulnerability in the io_uring subsystem, it is possible to leak kernel memory information to the user process. timens_install calls current_is_single_threaded to determine if the current process is single-threaded, but this call does not consider io_uring's io_worker threads, thus it is possible to insert a time namespace's vvar page to process's memory space via a page fault. When this time namespace is destroyed, the vvar page is also freed, but not removed from the process' memory, and a next page allocated by the kernel will be still available from the user-space process and can leak memory contents via this (read-only) use-after-free vulnerability. We recommend upgrading past version 5.10.161 or commit 788d0824269bef539fe31a785b1517882eafed93 https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/io_uring | 5.5 | More Details |
| CVE-2023-24809 | NetHack is a single player dungeon exploration game. Starting with version 3.6.2 and prior to version 3.6.7, illegal input to the "C" (call) command can cause a buffer overflow and crash the NetHack process. This vulnerability may be a security issue for systems that have NetHack installed suid/sgid and for shared systems. For all systems, it may result in a process crash. This issue is resolved in NetHack 3.6.7. There are no known workarounds. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-21577 | Photoshop version 23.5.3 (and earlier), 24.1 (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 | More Details |
| CVE-2023-21578 | Photoshop version 23.5.3 (and earlier), 24.1 (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 | More Details |
| CVE-2023-20949 | In s2mpg11_pmic_probe of s2mpg11-regulator.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 kernelAndroid ID: A-259323133References: N/A | 5.5 | More Details |
| CVE-2023-21583 | Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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 | More Details |
| CVE-2023-21584 | FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are 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 | More Details |
| CVE-2023-21593 | Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 5.5 | More Details |
| CVE-2023-21620 | FrameMaker 2020 Update 4 (and earlier), 2022 (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 | More Details |
| CVE-2022-4785 | The Video Sidebar Widgets WordPress plugin through 6.1 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 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-4786 | The Video.js WordPress plugin through 4.5.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2022-4791 | The Product Slider and Carousel with Category for WooCommerce WordPress plugin before 2.8 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack. | 5.4 | More Details |
| CVE-2023-0419 | The Shortcode for Font Awesome WordPress plugin before 1.4.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2023-0371 | The EmbedSocial WordPress plugin before 1.1.28 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 | More Details |
| CVE-2023-0372 | The EmbedStories WordPress plugin before 0.7.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2022-48320 | Cross-site Request Forgery (CSRF) in Tribe29's Checkmk <= 2.1.0p17, Checkmk <= 2.0.0p31, and all versions of Checkmk 1.6.0 (EOL) allow an attacker to add new visual elements to multiple pages. | 5.4 | More Details |
| CVE-2023-0059 | The Youzify WordPress plugin before 1.2.2 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 | More Details |
| CVE-2023-0067 | The Timed Content WordPress plugin before 2.73 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 | More Details |
| CVE-2023-0231 | The ShopLentor WordPress plugin before 2.5.4 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 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-4777 | The Bootstrap Shortcodes WordPress plugin through 3.4.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2023-0271 | The WP Font Awesome WordPress plugin before 1.7.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2023-0285 | The Real Media Library WordPress plugin before 4.18.29 does not sanitise and escape the created folder names, which could allow users with the role of author and above to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2023-0380 | The Easy Digital Downloads WordPress plugin before 3.1.0.5 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 | More Details |
| CVE-2022-4784 | The Hueman Addons WordPress plugin through 2.3.3 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 | More Details |
| CVE-2021-32852 | Countly, a product analytics solution, is vulnerable to cross-site scripting prior to version 21.11 of the community edition. The victim must follow a malicious link or be redirected there from malicious web site. The attacker must have an account or be able to create one. This issue is patched in version 21.11. | 5.4 | More Details |
| CVE-2022-4764 | The Simple File Downloader WordPress plugin through 1.0.4 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 | More Details |
| CVE-2022-4761 | The Post Views Count WordPress plugin through 3.0.2 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 | More Details |
| CVE-2023-0934 | Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.5. | 5.4 | More Details |
| CVE-2023-0559 | The GS Portfolio for Envato WordPress plugin before 1.4.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-36656 | The Spectra WordPress plugin before 1.15.0 does not sanitize user input as it reaches its style HTML attribute, allowing contributors to conduct stored XSS attacks via the plugin's Gutenberg blocks. | 5.4 | More Details |
| CVE-2023-0375 | The Easy Affiliate Links WordPress plugin before 3.7.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2023-0541 | The GS Books Showcase WordPress plugin before 1.3.1 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 | More Details |
| CVE-2023-0366 | The Loan Comparison WordPress plugin before 1.5.3 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 | More Details |
| CVE-2022-4666 | The Markup (JSON-LD) structured in schema.org WordPress plugin through 4.8.1 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 | More Details |
| CVE-2022-4669 | The Page Builder: Live Composer WordPress plugin before 1.5.23 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 | More Details |
| CVE-2022-4714 | The WP Dark Mode WordPress plugin before 4.0.0 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack | 5.4 | More Details |
| CVE-2023-0540 | The GS Filterable Portfolio WordPress plugin before 1.6.1 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 | More Details |
| CVE-2022-4750 | The WP Responsive Testimonials Slider And Widget WordPress plugin through 1.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0492 | The GS Products Slider for WooCommerce WordPress plugin before 1.5.9 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 | More Details |
| CVE-2023-0378 | The Greenshift WordPress plugin before 5.0 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 | More Details |
| CVE-2022-4752 | The Opening Hours WordPress plugin through 2.3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks | 5.4 | More Details |
| CVE-2022-4754 | The Easy Social Box / Page Plugin WordPress plugin through 4.1.2 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 | More Details |
| CVE-2022-4622 | The Login Logout Menu WordPress plugin through 1.3.3 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 | More Details |
| CVE-2023-24388 | Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Booking calendar, Appointment Booking System plugin <= 3.2.3 versions affects plugin forms actions (create, duplicate, edit, delete). | 5.4 | More Details |
| CVE-2023-24081 | Multiple stored cross-site scripting (XSS) vulnerabilities in Redrock Software TutorTrac before v4.2.170210 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the reason and location fields of the visits listing page. | 5.4 | More Details |
| CVE-2023-25764 | Jenkins Email Extension Plugin 2.93 and earlier does not escape, sanitize, or sandbox rendered email template output or log output generated during template rendering, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create or change custom email templates. | 5.4 | More Details |
| CVE-2021-40555 | Cross site scripting (XSS) vulnerability in flatCore-CMS 2.2.15 allows attackers to execute arbitrary code via description field on the new page creation form. | 5.4 | More Details |
| CVE-2022-40348 | Cross Site Scripting (XSS) vulnerability in Intern Record System version 1.0 in /intern/controller.php in 'name' and 'email' parameters, allows attackers to execute arbitrary code. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-25978 | All versions of the package github.com/usememos/memos/server are vulnerable to Cross-site Scripting (XSS) due to insufficient checks on external resources, which allows malicious actors to introduce links starting with a javascript: scheme. | 5.4 | More Details |
| CVE-2023-22868 | IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. | 5.4 | More Details |
| CVE-2023-24769 | Changedetection.io before v0.40.1.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the main page. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the URL parameter under the "Add a new change detection watch" function. | 5.4 | More Details |
| CVE-2023-25763 | Jenkins Email Extension Plugin 2.93 and earlier does not escape various fields included in bundled email templates, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control affected fields. | 5.4 | More Details |
| CVE-2023-25762 | Jenkins Pipeline: Build Step Plugin 2.18 and earlier does not escape job names in a JavaScript expression used in the Pipeline Snippet Generator, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control job names. | 5.4 | More Details |
| CVE-2023-25761 | Jenkins JUnit Plugin 1166.va_436e268e972 and earlier does not escape test case class names in JavaScript expressions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control test case class names in the JUnit resources processed by the plugin. | 5.4 | More Details |
| CVE-2023-0848 | A vulnerability was found in Netgear WNDR3700v2 1.0.1.14. It has been rated as problematic. This issue affects some unknown processing of the component Web Management Interface. The manipulation leads to denial of service. 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-221147. | 5.3 | More Details |
| CVE-2022-27891 | Palantir Gotham included an unauthenticated endpoint that listed all active usernames on the stack with an active session. The affected services have been patched and automatically deployed to all Apollo-managed Gotham instances. It is highly recommended that customers upgrade all affected services to the latest version. This issue affects: Palantir Gotham versions prior to 103.30221005.0. | 5.3 | More Details |
| CVE-2023-23463 | Sunell DVR, latest version, Insufficiently Protected Credentials (CWE-522) may be exposed through an unspecified request. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-27892 | Palantir Gotham versions prior to 3.22.11.2 included an unauthenticated endpoint that would have allowed an attacker to exhaust the memory of the Gotham dispatch service. | 5.3 | More Details |
| CVE-2022-27897 | Palantir Gotham versions prior to 3.22.11.2 included an unauthenticated endpoint that would load portions of maliciously crafted zip files to memory. An attacker could repeatedly upload a malicious zip file, which would allow them to exhaust memory resources on the dispatch server. | 5.3 | More Details |
| CVE-2021-32419 | An issue in Schism Tracker v20200412 fixed in v.20200412 allows attacker to obtain sensitive information via the fmt_mtm_load_song function in fmt/mtm.c. | 5.3 | More Details |
| CVE-2022-41734 | IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 237587. | 5.3 | More Details |
| CVE-2023-22580 | Due to improper input filtering in the sequalize js library, can malicious queries lead to sensitive information disclosure. | 5.3 | More Details |
| CVE-2023-25173 | containerd is an open source container runtime. A bug was found in containerd prior to versions 1.6.18 and 1.5.18 where supplementary groups are not set up properly inside a container. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that container. Downstream applications that use the containerd client library may be affected as well. This bug has been fixed in containerd v1.6.18 and v.1.5.18. Users should update to these versions and recreate containers to resolve this issue. Users who rely on a downstream application that uses containerd's client library should check that application for a separate advisory and instructions. As a workaround, ensure that the `"USER $USERNAME"` Dockerfile instruction is not used. Instead, set the container entrypoint to a value similar to `ENTRYPOINT ["su", "-", "user"]` to allow `su` to properly set up supplementary groups. | 5.3 | More Details |
| CVE-2022-30299 | A path traversal vulnerability [CWE-23] in the API of FortiWeb 7.0.0 through 7.0.1, 6.3.0 through 6.3.19, 6.4 all versions, 6.2 all versions, 6.1 all versions, 6.0 all versions may allow an authenticated attacker to retrieve specific parts of files from the underlying file system via specially crafted web requests. | 5.3 | More Details |
| CVE-2023-26265 | The Borg theme before 1.1.19 for Backdrop CMS does not sufficiently sanitize path arguments that are passed in via a URL. The function borg_preprocess_page in the file template.php does not properly sanitize incoming path arguments before using them. | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2016-15026 | A vulnerability was found in 3breadt dd-plist 1.17 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to xml external entity reference. An attack has to be approached locally. Upgrading to version 1.18 is able to address this issue. The patch is identified as 8c954e8d9f6f6863729e50105a8abf3f87fff74c. It is recommended to upgrade the affected component. VDB-221486 is the identifier assigned to this vulnerability. | 5.3 | More Details |
| CVE-2023-22232 | Adobe Connect versions 11.4.5 (and earlier), 12.1.5 (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 integrity of a minor feature. Exploitation of this issue does not require user interaction. | 5.3 | More Details |
| CVE-2023-0901 | Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository pixelfed/pixelfed prior to 0.11.4. | 5.3 | More Details |
| CVE-2022-48318 | No authorisation controls in the RestAPI documentation for Tribe29's Checkmk <= 2.1.0p13 and Checkmk <= 2.0.0p29 which may lead to unintended information disclosure through automatically generated user specific tags within Rest API documentation. | 5.3 | More Details |
| CVE-2023-25192 | AMI MegaRAC SPX devices allow User Enumeration through Redfish. The fixed versions are SPx12-update-7.00 and SPx13-update-5.00. | 5.3 | More Details |
| CVE-2023-23752 | An issue was discovered in Joomla! 4.0.0 through 4.2.7. An improper access check allows unauthorized access to webservice endpoints. | 5.3 | More Details |
| CVE-2023-0914 | Improper Authorization in GitHub repository pixelfed/pixelfed prior to 0.11.4. | 5.3 | More Details |
| CVE-2023-0903 | A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file edit-task.php. The manipulation of the argument task_id leads to sql injection. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221452. | 5.0 | More Details |
| CVE-2023-23778 | A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. | 4.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-44299 | SiteServerCMS 7.1.3 sscms has a file read vulnerability. | 4.9 | More Details |
| CVE-2022-43929 | IBM Db2 for Linux, UNIX and Windows 11.1 and 11.5 may be vulnerable to a Denial of Service when executing a specially crafted 'Load' command. IBM X-Force ID: 241676. | 4.9 | More Details |
| CVE-2022-34843 | Integer overflow in the Intel(R) Trace Analyzer and Collector software before version 2021.5 may allow an authenticated user to potentially enable escalation of privilege via local access. | 4.8 | More Details |
| CVE-2022-32575 | Out-of-bounds write in the Intel(R) Trace Analyzer and Collector software before version 2021.5 may allow an authenticated user to potentially enable escalation of privilege via local access. | 4.8 | More Details |
| CVE-2022-34346 | Out-of-bounds read in the Intel(R) Media SDK software before version 22.2.2 may allow an authenticated user to potentially enable escalation of privilege via local access. | 4.8 | More Details |
| CVE-2022-39948 | An improper certificate validation vulnerability [CWE-295] in FortiOS 7.2.0 through 7.2.3, 7.0.0 through 7.0.7, 6.4 all versions, 6.2 all versions, 6.0 all versions and FortiProxy 7.0.0 through 7.0.6, 2.0 all versions, 1.2 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the FortiOS/FortiProxy device and remote servers hosting threat feeds (when the latter are configured as Fabric connectors in FortiOS/FortiProxy) | 4.8 | More Details |
| CVE-2023-0429 | The Watu Quiz WordPress plugin before 3.3.8.2 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 | More Details |
| CVE-2023-0849 | A vulnerability has been found in Netgear WNDR3700v2 1.0.1.14 and classified as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to command 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-221152. | 4.7 | More Details |
| CVE-2023-0943 | A vulnerability, which was classified as problematic, has been found in SourceCodester Best POS Management System 1.0. This issue affects the function save_settings of the file index.php?page=site_settings of the component Image Handler. The manipulation of the argument img with the input ../../shell.php leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221591. | 4.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0913 | A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. This vulnerability affects unknown code of the file /adms/admin/?page=vehicles/sell_vehicle. 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-221482 is the identifier assigned to this vulnerability. | 4.7 | More Details |
| CVE-2023-0912 | A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page=vehicles/view_transaction. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221481 was assigned to this vulnerability. | 4.7 | More Details |
| CVE-2023-25928 | IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. | 4.6 | More Details |
| CVE-2022-43579 | IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.7 and 6.1.0.0 through 6.1.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 238684. | 4.6 | More Details |
| CVE-2022-29493 | Uncaught exception in webserver for the Integrated BMC in some Intel(R) platforms before versions 2.86, 2.09 and 2.78 may allow a privileged user to potentially enable denial of service via network access. | 4.5 | More Details |
| CVE-2022-34849 | Uncaught exception in the Intel(R) Iris(R) Xe MAX drivers for Windows before version 100.0.5.1436(v2) may allow a privileged user to potentially enable denial of service via local access. | 4.4 | More Details |
| CVE-2022-30531 | Out-of-bounds read in the Intel(R) Iris(R) Xe MAX drivers for Windows before version 100.0.5.1474 may allow a privileged user to potentially enable information disclosure via local access. | 4.4 | More Details |
| CVE-2022-45154 | A Cleartext Storage of Sensitive Information vulnerability in suppportutils of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15, SUSE Linux Enterprise Server 15 SP3 allows attackers that get access to the support logs to gain knowledge of the stored credentials This issue affects: SUSE Linux Enterprise Server 12 supportutils version 3.0.10-95.51.1CWE-312: Cleartext Storage of Sensitive Information and prior versions. SUSE Linux Enterprise Server 15 supportutils version 3.1.21-150000.5.44.1 and prior versions. SUSE Linux Enterprise Server 15 SP3 supportutils version 3.1.21-150300.7.35.15.1 and prior versions. | 4.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-36416 | Protection mechanism failure in the Intel(R) Ethernet 500 Series Controller drivers for VMware before version 1.10.0.13 may allow an authenticated user to potentially enable escalation of privilege via local access. | 4.4 | More Details |
| CVE-2023-0907 | A vulnerability, which was classified as problematic, has been found in Filseclab Twister Antivirus 8.17. Affected by this issue is the function 0x220017 in the library ffsmon.sys of the component IoControlCode 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 of this vulnerability is VDB-221456. | 4.4 | More Details |
| CVE-2022-38731 | Qaelum DOSE 18.08 through 21.1 before 21.2 allows Directory Traversal via the loadimages name parameter. It allows a user to specify an arbitrary location on the server's filesystem from which to load an image. (Only images are displayed to the attacker. All other files are loaded but not displayed.) The Content-Type response header reflects the actual content type of the file being requested. This allows an attacker to enumerate files on the local system. Additionally, remote resources can be requested via a UNC path, allowing an attacker to coerce authentication out from the server to the attackers machine. | 4.3 | More Details |
| CVE-2015-10081 | A vulnerability was found in arnoldle submitByMailPlugin 1.0b2.9 and classified as problematic. This issue affects some unknown processing of the file edit_list.php. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. Upgrading to version 1.0b2.9a is able to address this issue. The patch is named a739f680a1623d22f52ff1371e86ca472e63756f. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-221495. | 4.3 | More Details |
| CVE-2021-43074 | An improper verification of cryptographic signature vulnerability [CWE-347] in FortiWeb 6.4 all versions, 6.3.16 and below, 6.2 all versions, 6.1 all versions, 6.0 all versions; FortiOS 7.0.3 and below, 6.4.8 and below, 6.2 all versions, 6.0 all versions; FortiSwitch 7.0.3 and below, 6.4.10 and below, 6.2 all versions, 6.0 all versions; FortiProxy 7.0.1 and below, 2.0.7 and below, 1.2 all versions, 1.1 all versions, 1.0 all versions may allow an attacker to decrypt portions of the administrative session management cookie if able to intercept the latter. | 4.3 | More Details |
| CVE-2023-25766 | A missing permission check in Jenkins Azure Credentials Plugin 253.v887e0f9e898b and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. | 4.3 | More Details |
| CVE-2023-0453 | The WP Private Message WordPress plugin (bundled with the Superio theme as a required plugin) before 1.0.6 does not ensure that private messages to be accessed belong to the user making the requests. This allowing any authenticated users to access private messages belonging to other users by tampering the ID. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-40231 | IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.7 and 6.1.0.0 through 6.1.2.0 could allow an authenticated user to perform unauthorized actions due to improper access controls. IBM X-Force ID: 235533. | 4.3 | More Details |
| CVE-2022-43954 | An insertion of sensitive information into log file vulnerability [CWE-532] in the FortiPortal management interface 7.0.0 through 7.0.2 may allow a remote authenticated attacker to read other devices' passwords in the audit log page. | 4.3 | More Details |
| CVE-2023-23848 | Missing permission checks in Synopsys Jenkins Coverity Plugin 3.0.2 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. | 4.3 | More Details |
| CVE-2022-27234 | Server-side request forgery in the CVAT software maintained by Intel(R) before version 2.0.1 may allow an authenticated user to potentially enable information disclosure via network access. | 4.3 | More Details |
| CVE-2022-4385 | The Intuitive Custom Post Order WordPress plugin before 3.1.4 does not check for authorization in the update-menu-order ajax action, allowing any logged in user (with roles as low as Subscriber) to update the menu order | 4.3 | More Details |
| CVE-2022-4386 | The Intuitive Custom Post Order WordPress plugin before 3.1.4 lacks CSRF protection in its update-menu-order ajax action, allowing an attacker to trick any user to change the menu order via a CSRF attack | 4.3 | More Details |
| CVE-2023-23899 | Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Extensions For CF7 plugin <= 2.0.8 versions leads to arbitrary plugin activation. | 4.3 | More Details |
| CVE-2023-23850 | A missing permission check in Synopsys Jenkins Coverity Plugin 3.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. | 4.3 | More Details |
| CVE-2023-24499 | Butterfly Button plugin may leave traces of its use on user's device. Since it is used for reporting domestic problems, this may lead to spouse knowing about its use. | 4.3 | More Details |
| CVE-2022-30304 | An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiAnalyzer versions prior to 7.2.1, 7.0.4 and 6.4.8 may allow a remote unauthenticated attacker to perform a stored cross site scripting (XSS) attack via the URL parameter observed in the FortiWeb attack event logview in FortiAnalyzer. | 4.3 | More Details |
| CVE-2023-0475 | HashiCorp go-getter up to 1.6.2 and 2.1.1 is vulnerable to decompression bombs. Fixed in 1.7.0 and 2.2.0. | 4.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-42472 | A improper neutralization of crlf sequences in http headers ('http response splitting') in Fortinet FortiOS versions 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.11, 6.2.0 through 6.2.12, 6.0.0 through 6.0.16, FortiProxy 7.2.0 through 7.2.1, 7.0.0 through 7.0.7, 2.0.0 through 2.0.10, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6 may allow an authenticated and remote attacker to perform an HTTP request splitting attack which gives attackers control of the remaining headers and body of the response. | 4.2 | More Details |
| CVE-2022-34864 | Out-of-bounds read in the Intel(R) Trace Analyzer and Collector software before version 2021.5 may allow an authenticated user to potentially enable escalation of privilege via local access. | 4.2 | More Details |
| CVE-2022-38378 | An improper privilege management vulnerability [CWE-269] in Fortinet FortiOS version 7.2.0 and before 7.0.7 and FortiProxy version 7.2.0 through 7.2.1 and before 7.0.7 allows an attacker that has access to the admin profile section (System subsection Administrator Users) to modify their own profile and upgrade their privileges to Read Write via CLI or GUI commands. | 4.2 | More Details |
| CVE-2022-36287 | Uncaught exception in the FCS Server software maintained by Intel before version 1.1.79.3 may allow a privileged user to potentially enable denial of service via physical access. | 4.0 | More Details |
| CVE-2022-38056 | Improper neutralization in the Intel(R) EMA software before version 1.8.1.0 may allow a privileged user to potentially enable escalation of privilege via network access. | 3.8 | More Details |
| CVE-2012-10007 | A vulnerability was found in madgicweb BuddyStream Plugin up to 3.2.7 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file ShareBox.php. The manipulation of the argument content/link/shares leads to cross site scripting. The attack can be launched remotely. Upgrading to version 3.2.8 is able to address this issue. The patch is named 7d5b9a89a27711aad76fd55ab4cc4185b545a1d0. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-221479. | 3.5 | More Details |
| CVE-2023-23847 | A cross-site request forgery (CSRF) vulnerability in Synopsys Jenkins Coverity Plugin 3.0.2 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. | 3.5 | More Details |
| CVE-2023-0840 | A vulnerability classified as problematic was found in PHPCrazy 1.1.1. This vulnerability affects unknown code of the file admin/admin.php?action=users&mode=info&user=2. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221086 is the identifier assigned to this vulnerability. | 3.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2016-15025 | A vulnerability, which was classified as problematic, was found in generator-hottowel 0.0.11. Affected is an unknown function of the file app/templates/src/server/_app.js of the component 404 Error Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is c17092fd4103143a9ddab93c8983ace8bf174396. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-221484. | 3.5 | More Details |
| CVE-2015-10080 | A vulnerability was found in NREL api-umbrella-web 0.7.1. It has been classified as problematic. This affects an unknown part of the component Admin Data Table Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 0.8.0 is able to address this issue. The patch is named f53a9fb87e10c457f0f3dd4f2af24d3b2f21b3ca. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-221487. | 3.5 | More Details |
| CVE-2014-125088 | A vulnerability was found in qt-users-jp silk 0.0.1. It has been declared as problematic. This vulnerability affects unknown code of the file contents/root/examples/header.qml. The manipulation of the argument model.key/model.value leads to cross site scripting. The attack can be initiated remotely. The name of the patch is bbc5d6eeea800025ef29edda3fd3c57836239eae. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-221488. | 3.5 | More Details |
| CVE-2019-25104 | A vulnerability has been found in rtcwcoop 1.0.2 and classified as problematic. Affected by this vulnerability is the function AICast_ScriptLoad of the file code/game/ai_cast_script.c of the component Team Command Handler. The manipulation leads to denial of service. The identifier of the patch is f2cd18bc2e1cbca8c4b78bee9c392272bd5f42ac. It is recommended to apply a patch to fix this issue. The identifier VDB-221485 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2023-0945 | A vulnerability, which was classified as problematic, was found in SourceCodester Best POS Management System 1.0. Affected is an unknown function of the file index.php?page=add-category. The manipulation of the argument Name with the input "><img src=x onerror=prompt(document.domain);> leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-221592. | 3.5 | More Details |
| CVE-2023-0902 | A vulnerability was found in SourceCodester Simple Food Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file process_order.php. The manipulation of the argument order leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221451. | 3.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2015-10085 | A vulnerability was found in GoPistolet. It has been declared as problematic. This vulnerability affects unknown code of the component MTA. The manipulation leads to denial of service. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as b91aa4674d460993765884e8463c70e6d886bc90. It is recommended to apply a patch to fix this issue. VDB-221506 is the identifier assigned to this vulnerability. | 3.5 | More Details |
| CVE-2014-125089 | A vulnerability was found in cention-chatserver 3.8.0-rc1. It has been declared as problematic. Affected by this vulnerability is the function _formatBody of the file lib/InternalChatProtocol.fe. The manipulation of the argument body leads to cross site scripting. The attack can be launched remotely. Upgrading to version 3.9 is able to address this issue. The identifier of the patch is c4c0258bbd18f6915f97f91d5fee625384096a26. It is recommended to upgrade the affected component. The identifier VDB-221497 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2016-15027 | A vulnerability was found in meta4creations Post Duplicator Plugin 2.18 on WordPress. It has been classified as problematic. Affected is the function mtphr_post_duplicator_notice of the file includes/notices.php. The manipulation of the argument post-duplicated leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.19 is able to address this issue. The name of the patch is ca67c05e490c0cf93a1e9b2d93bfeff3dd96f594. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-221496. | 3.5 | More Details |
| CVE-2022-29054 | A missing cryptographic steps vulnerability [CWE-325] in the functions that encrypt the DHCP and DNS keys in Fortinet FortiOS version 7.2.0, 7.0.0 through 7.0.5, 6.4.0 through 6.4.9, 6.2.x and 6.0.x may allow an attacker in possession of the encrypted key to decipher it. | 3.3 | More Details |
| CVE-2022-36797 | Protection mechanism failure in the Intel(R) Ethernet 500 Series Controller drivers for VMware before version 1.10.0.1 may allow an authenticated user to potentially enable denial of service via local access. | 3.3 | More Details |
| CVE-2022-29523 | Improper conditions check in the Open CAS software maintained by Intel(R) before version 22.3.1 may allow an authenticated user to potentially enable denial of service via local access. | 3.3 | More Details |
| CVE-2023-0909 | A vulnerability, which was classified as problematic, was found in cxasm notepad-- 1.22. This affects an unknown part of the component Directory Comparison Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The associated identifier of this vulnerability is VDB-221475. | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-0187 | Improper access control in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access. | 3.2 | More Details |
| CVE-2022-32971 | Improper authentication in the Intel(R) SUR software before version 2.4.8902 may allow a privileged user to potentially enable escalation of privilege via network access. | 3.1 | More Details |
| CVE-2017-20178 | ** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Codiad 2.8.0. It has been rated as problematic. Affected by this issue is the function saveJSON of the file components/install/process.php. The manipulation of the argument data leads to information disclosure. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 2.8.1 is able to address this issue. The patch is identified as 517119de673e62547ee472a730be0604f44342b5. It is recommended to upgrade the affected component. VDB-221498 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. | 3.1 | More Details |
| CVE-2022-26888 | Cross-site scripting in the Intel(R) Quartus Prime Pro and Standard edition software may allow an authenticated user to potentially enable information disclosure via local access. | 2.8 | More Details |
| CVE-2022-36289 | Protection mechanism failure in the Intel(R) Media SDK software before version 22.2.2 may allow an authenticated user to potentially enable denial of service via local access. | 2.8 | More Details |
| CVE-2023-0850 | A vulnerability was found in Netgear WNDR3700v2 1.0.1.14 and classified as problematic. This issue affects some unknown processing of the component Web Interface. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221153 was assigned to this vulnerability. | 2.7 | More Details |
| CVE-2016-15024 | A vulnerability was found in doomsider shadow. It has been classified as problematic. Affected is an unknown function. The manipulation leads to denial of service. Attacking locally is a requirement. The complexity of an attack is rather high. The exploitability is told to be difficult. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as 3332c5ba9ec3014ddc74e2147190a050eee97bc0. It is recommended to apply a patch to fix this issue. VDB-221478 is the identifier assigned to this vulnerability. | 2.5 | More Details |
| CVE-2022-26841 | Insufficient control flow management for the Intel(R) SGX SDK software for Linux before version 2.16.100.1 may allow an authenticated user to potentially enable information disclosure via local access. | 2.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-26509 | Improper conditions check in the Intel(R) SGX SDK software may allow a privileged user to potentially enable information disclosure via local access. | 2.5 | More Details |
| CVE-2022-35883 | NULL pointer dereference in the Intel(R) Media SDK software before version 22.2.2 may allow an authenticated user to potentially enable denial of service via local access. | 2.2 | More Details |
| CVE-2021-23945 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23952 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23951 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23950 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23949 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23948 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23947 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23946 | 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. Notes: none. | N/A | More Details |
| CVE-2021-33237 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Consult IDs: CVE-2021-36686. Reason: This candidate is a duplicate of CVE-2021-36686. Notes: All CVE users should reference CVE-2021-36686 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage. | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-23944 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23943 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23942 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23941 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23940 | 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. Notes: none. | N/A | More Details |
| CVE-2021-23939 | 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. Notes: none. | N/A | More Details |
| CVE-2021-32861 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-32856. Reason: This candidate is a reservation duplicate of CVE-2021-32856. Notes: All CVE users should reference CVE-2021-32856 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage. | N/A | More Details |
| CVE-2021-23938 | 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. Notes: none. | N/A | More Details |