SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 12 April 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-2023-29017 | vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. Prior to version 3.9.15, vm2 was not properly handling host objects passed to `Error.prepareStackTrace` in case of unhandled async errors. A threat actor could bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version 3.9.15 of vm2. There are no known workarounds. | 10.0 | More Details |
| CVE-2023-28849 | GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.7, GLPI inventory endpoint can be used to drive a SQL injection attack. It can also be used to store malicious code that could be used to perform XSS attack. By default, GLPI inventory endpoint requires no authentication. Version 10.0.7 contains a patch for this issue. As a workaround, disable native inventory. | 10.0 | More Details |
| CVE-2023-27497 | Due to missing authentication and input sanitization of code the EventLogServiceCollector of SAP Diagnostics Agent - version 720, allows an attacker to execute malicious scripts on all connected Diagnostics Agents running on Windows. On successful exploitation, the attacker can completely compromise confidentiality, integrity and availability of the system. | 10.0 | More Details |
| CVE-2022-41976 | An privilege escalation issue was discovered in Scada-LTS 2.7.1.1 build 2948559113 allows remote attackers, authenticated in the application as a low-privileged user to change role (e.g., to administrator) by updating their user profile. | 9.9 | More Details |
| CVE-2023-1782 | HashiCorp Nomad and Nomad Enterprise versions 1.5.0 up to 1.5.2 allow unauthenticated users to bypass intended ACL authorizations for clusters where mTLS is not enabled. This issue is fixed in version 1.5.3. | 9.9 | More Details |
| CVE-2023-29374 | In LangChain through 0.0.131, the LLMMathChain chain allows prompt injection attacks that can execute arbitrary code via the Python exec method. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27650 | An issue found in APUS Group Launcher v.3.10.73 and v.3.10.88 allows a remote attacker to execute arbitrary code via the FONT_FILE parameter. | 9.8 | More Details |
| CVE-2023-29375 | An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potentially dangerous file upload through the SharePoint connector. | 9.8 | More Details |
| CVE-2023-1478 | The Hummingbird WordPress plugin before 3.4.2 does not validate the generated file path for page cache files before writing them, leading to a path traversal vulnerability in the page cache module. | 9.8 | More Details |
| CVE-2023-29216 | In Apache Linkis <=1.3.1, because the parameters are not effectively filtered, the attacker uses the MySQL data source and malicious parameters to configure a new data source to trigger a deserialization vulnerability, eventually leading to remote code execution. Versions of Apache Linkis <= 1.3.0 will be affected. We recommend users upgrade the version of Linkis to version 1.3.2. | 9.8 | More Details |
| CVE-2023-29215 | In Apache Linkis <=1.3.1, due to the lack of effective filtering of parameters, an attacker configuring malicious Mysql JDBC parameters in JDBC EengineConn Module will trigger a deserialization vulnerability and eventually lead to remote code execution. Therefore, the parameters in the Mysql JDBC URL should be blacklisted. Versions of Apache Linkis <= 1.3.0 will be affected. We recommend users upgrade the version of Linkis to version 1.3.2. | 9.8 | More Details |
| CVE-2023-27603 | In Apache Linkis <=1.3.1, due to the Manager module engineConn material upload does not check the zip path, This is a Zip Slip issue, which will lead to a potential RCE vulnerability. We recommend users upgrade the version of Linkis to version 1.3.2. | 9.8 | More Details |
| CVE-2023-27602 | In Apache Linkis <=1.3.1, The PublicService module uploads files without restrictions on the path to the uploaded files, and file types. We recommend users upgrade the version of Linkis to version 1.3.2.  For versions <=1.3.1, we suggest turning on the file path check switch in linkis.properties `wds.linkis.workspace.filesystem.owner.check=true` `wds.linkis.workspace.filesystem.path.check=true` | 9.8 | More Details |
| CVE-2023-26063 | Certain Lexmark devices through 2023-02-19 access a Resource By Using an Incompatible Type. | 9.8 | More Details |
| CVE-2023-27720 | D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_48d630 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27719 | D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_478360 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27718 | D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_498308 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27033 | Prestashop cdesigner v3.1.3 to v3.1.8 was discovered to contain a code injection vulnerability via the component CdesignerSaverotateModuleFrontController::initContent(). | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28706 | Improper Control of Generation of Code ('Code Injection') vulnerability in Apache Software Foundation Apache Airflow Hive Provider.This issue affects Apache Airflow Hive Provider: before 6.0.0. | 9.8 | More Details |
| CVE-2023-29478 | BiblioCraft before 2.4.6 does not sanitize path-traversal characters in filenames, allowing restricted write access to almost anywhere on the filesystem. This includes the Minecraft mods folder, which results in code execution. | 9.8 | More Details |
| CVE-2023-26978 | TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the pppoeAcName parameter at /setting/setWanIeCfg. | 9.8 | More Details |
| CVE-2022-46709 | A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13, iOS 16. An app may be able to execute arbitrary code with kernel privileges | 9.8 | More Details |
| CVE-2023-26066 | Certain Lexmark devices through 2023-02-19 have Improper Validation of an Array Index. | 9.8 | More Details |
| CVE-2023-26064 | Certain Lexmark devices through 2023-02-19 have an Out-of-bounds Write. | 9.8 | More Details |
| CVE-2023-26065 | Certain Lexmark devices through 2023-02-19 have an Integer Overflow. | 9.8 | More Details |
| CVE-2023-28250 | Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability | 9.8 | More Details |
| CVE-2023-21554 | Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability | 9.8 | More Details |
| CVE-2020-19802 | File Upload vulnerability found in Milken DoyoCMS v.2.3 allows a remote attacker to execute arbitrary code via the upload file type parameter. | 9.8 | More Details |
| CVE-2022-41331 | A missing authentication for critical function vulnerability [CWE-306] in FortiPresence infrastructure server before version 1.2.1 allows a remote, unauthenticated attacker to access the Redis and MongoDB instances via crafted authentication requests. | 9.8 | More Details |
| CVE-2023-27192 | An issue found in DUALSPACE Super Secuirty v.2.3.7 allows an attacker to cause a denial of service via the key_wifi_safe_net_check_url, KEY_Cirus_scan_whitelist and KEY_AD_NEW_USER_AVOID_TIME parameters. | 9.8 | More Details |
| CVE-2023-27645 | An issue found in POWERAMP audioplayer build 925 bundle play and build 954 allows a remote attacker to gain privileges via the reverb and EQ preset parameters. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28489 | A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05), CP-8050 MASTER MODULE (All versions < CPCI85 V05). Affected devices are vulnerable to command injection via the web server port 443/tcp, if the parameter “Remote Operation” is enabled. The parameter is disabled by default. The vulnerability could allow an unauthenticated remote attacker to perform arbitrary code execution on the device. | 9.8 | More Details |
| CVE-2023-29492 | Novi Survey before 8.9.43676 allows remote attackers to execute arbitrary code on the server in the context of the service account. This does not provide access to stored survey or response data. | 9.8 | More Details |
| CVE-2023-28765 | An attacker with basic privileges in SAP BusinessObjects Business Intelligence Platform (Promotion Management) - versions 420, 430, can get access to lcmbiar file and further decrypt the file. After this attacker can gain access to BI user’s passwords and depending on the privileges of the BI user, the attacker can perform operations that can completely compromise the application. | 9.8 | More Details |
| CVE-2023-27178 | An arbitrary file upload vulnerability in the upload function of GDidees CMS 3.9.1 allows attackers to execute arbitrary code via a crafted file. | 9.8 | More Details |
| CVE-2023-27076 | Command injection vulnerability found in Tenda G103 v.1.0.0.5 allows attacker to execute arbitrary code via a the language parameter. | 9.8 | More Details |
| CVE-2023-26070 | Certain Lexmark devices through 2023-02-19 mishandle Input Validation (issue 4 of 4). | 9.8 | More Details |
| CVE-2023-26069 | Certain Lexmark devices through 2023-02-19 mishandle Input Validation (issue 3 of 4). | 9.8 | More Details |
| CVE-2023-26068 | Certain Lexmark devices through 2023-02-19 mishandle Input Validation (issue 2 of 4). | 9.8 | More Details |
| CVE-2023-27021 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the formSetFirewallCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-26848 | TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the org parameter at setting/delStaticDhcpRules. | 9.8 | More Details |
| CVE-2023-27020 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25330 | A SQL injection vulnerability in Mybatis plus below 3.5.3.1 allows remote attackers to execute arbitrary SQL commands via the tenant ID valuer. NOTE: the vendor's position is that this can only occur in a misconfigured application; the documentation discusses how to develop applications that avoid SQL injection. | 9.8 | More Details |
| CVE-2023-27019 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_458FBC function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-24800 | D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_495220 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-24799 | D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_48AF78 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-24798 | D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_475FB0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-24797 | D-Link DIR882 DIR882A1_FW110B02 was discovered to contain a stack overflow in the sub_48AC20 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-29475 | inventory in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23543. | 9.8 | More Details |
| CVE-2023-29474 | inventory in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23552. | 9.8 | More Details |
| CVE-2023-29473 | webservice in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23710. | 9.8 | More Details |
| CVE-2023-28500 | A Java insecure deserialization vulnerability in Adobe LiveCycle ES4 version 11.0 and earlier allows unauthenticated remote attackers to gain operating system code execution by submitting specially crafted Java serialized objects to a specific URL. Adobe LiveCycle ES4 version 11.0.1 and later may be vulnerable if the application is installed with Java environment 7u21 and earlier. Exploitation of the vulnerability depends on two factors: insecure deserialization methods used in the Adobe LiveCycle application, and the use of Java environments 7u21 and earlier. The code execution is performed in the context of the account that is running the Adobe LiveCycle application. If the account is privileged, exploitation provides privileged access to the operating system. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. | 9.8 | More Details |
| CVE-2023-24538 | Templates do not properly consider backticks (`) as Javascript string delimiters, and do not escape them as expected. Backticks are used, since ES6, for JS template literals. If a template contains a Go template action within a Javascript template literal, the contents of the action can be used to terminate the literal, injecting arbitrary Javascript code into the Go template. As ES6 template literals are rather complex, and themselves can do string interpolation, the decision was made to simply disallow Go template actions from being used inside of them (e.g. "var a = {{.}}"), since there is no obviously safe way to allow this behavior. This takes the same approach as github.com/google/safehtml. With fix, Template.Parse returns an Error when it encounters templates like this, with an ErrorCode of value 12. This ErrorCode is currently unexported, but will be exported in the release of Go 1.21. Users who rely on the previous behavior can re-enable it using the GODEBUG flag jstmpllitinterp=1, with the caveat that backticks will now be escaped. This should be used with caution. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0750 | Yellobrik PEC-1864 implements authentication checks via javascript in the frontend interface. When the device can be accessed over the network an attacker could bypass authentication. This would allow an attacker to : - Change the password, resulting in a DOS of the users - Change the streaming source, compromising the integrity of the stream - Change the streaming destination, compromising the confidentiality of the stream This issue affects Yellowbrik: PEC 1864. No patch has been issued by the manufacturer as this model was discontinued. | 9.8 | More Details |
| CVE-2022-31890 | SQL Injection vulnerability in audit/class.audit.php in osTicket osTicket-plugins before commit a7842d494889fd5533d13deb3c6a7789768795ae via the order parameter to the getOrder function. | 9.8 | More Details |
| CVE-2023-24720 | An arbitrary file upload vulnerability in readium-js v0.32.0 allows attackers to execute arbitrary code via uploading a crafted EPUB file. | 9.8 | More Details |
| CVE-2022-4939 | THe WCFM Membership plugin for WordPress is vulnerable to privilege escalation in versions up to, and including 2.10.0, due to a missing capability check on the wp_ajax_nopriv_wcfm_ajax_controller AJAX action that controls membership settings. This makes it possible for unauthenticated attackers to modify the membership registration form in a way that allows them to set the role for registration to that of any user including administrators. Once configured, the attacker can then register as an administrator. | 9.8 | More Details |
| CVE-2023-1877 | Command Injection in GitHub repository microweber/microweber prior to 1.3.3. | 9.8 | More Details |
| CVE-2023-1788 | Insufficient Session Expiration in GitHub repository firefly-iii/firefly-iii prior to 6. | 9.8 | More Details |
| CVE-2023-25210 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromSetSysTime function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25211 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25212 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromSetWirelessRepeat function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25213 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the check_param_changed function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27018 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_45EC1C function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27017 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_45DC58 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27016 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27015 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_4A75C0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27014 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_46AC38 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27013 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the get_parentControl_list_Info function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-27012 | Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the setSchedWifi function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25220 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the add_white_node function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25219 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromDhcpListClient function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25218 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the form_fast_setting_wifi_set function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25217 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the formWifiBasicSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25216 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the formSetFirewallCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25215 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-25214 | Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the setSchedWifi function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. | 9.8 | More Details |
| CVE-2023-28838 | GLPI is a free asset and IT management software package. Starting in version 0.50 and prior to versions 9.5.13 and 10.0.7, a SQL Injection vulnerability allow users with access rights to statistics or reports to extract all data from database and, in some cases, write a webshell on the server. Versions 9.5.13 and 10.0.7 contain a patch for this issue. As a workaround, remove `Assistance > Statistics` and `Tools > Reports` read rights from every user. | 9.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27987 | In Apache Linkis <=1.3.1, due to the default token generated by Linkis Gateway deployment being too simple, it is easy for attackers to obtain the default token for the attack. Generation rules should add random values. We recommend users upgrade the version of Linkis to version 1.3.2 And modify the default token value. You can refer to Token authorization[1] https://linkis.apache.org/docs/latest/auth/token https://linkis.apache.org/docs/latest/auth/token | 9.1 | More Details |
| CVE-2023-28808 | Some Hikvision Hybrid SAN/Cluster Storage products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices. | 9.1 | More Details |
| CVE-2023-27267 | Due to missing authentication and insufficient input validation, the OSCommand Bridge of SAP Diagnostics Agent - version 720, allows an attacker with deep knowledge of the system to execute scripts on all connected Diagnostics Agents. On successful exploitation, the attacker can completely compromise confidentiality, integrity and availability of the system. | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-22613 | An issue was discovered in IhisiSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. It is possible to write to an attacker-controlled address. An attacker could invoke an SMI handler with a malformed pointer in RCX that overlaps SMRAM, resulting in SMM memory corruption. | 8.8 | More Details |
| CVE-2023-24926 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-22612 | An issue was discovered in IhisiSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. A malicious host OS can invoke an Insyde SMI handler with malformed arguments, resulting in memory corruption in SMM. | 8.8 | More Details |
| CVE-2023-22614 | An issue was discovered in ChipsetSvcSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. There is insufficient input validation in BIOS Guard updates. An attacker can induce memory corruption in SMM by supplying malformed inputs to the BIOS Guard SMI handler. | 8.8 | More Details |
| CVE-2023-24884 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24885 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24886 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24887 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24924 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-24925 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24927 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-28243 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24928 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-24929 | Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-20102 | A vulnerability in the web-based management interface of Cisco Secure Network Analytics could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system. This vulnerability is due to insufficient sanitization of user-provided data that is parsed into system memory. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the administrator user. | 8.8 | More Details |
| CVE-2023-1522 | SQL Injection in the Hardware Inventory report of Security Center 5.11.2. | 8.8 | More Details |
| CVE-2023-29006 | The Order GLPI plugin allows users to manage order management within GLPI. Starting with version 1.8.0 and prior to versions 2.7.7 and 2.10.1, an authenticated user that has access to standard interface can craft an URL that can be used to execute a system command. Versions 2.7.7 and 2.10.1 contain a patch for this issue. As a workaround, delete the `ajax/dropdownContact.php` file from the plugin. | 8.8 | More Details |
| CVE-2023-28231 | DHCP Server Service Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2022-4935 | The WCFM Marketplace plugin for WordPress is vulnerable to unauthorized modification and access of data in versions up to, and including, 3.4.11 due to missing capability checks on various AJAX actions. This makes it possible for authenticated attackers, with minimal permissions such as subscribers, to perform a wide variety of actions such as modifying shipping method details, modifying products, deleting arbitrary posts, and privilege escalation (via the wp_ajax_wcfm_vendor_store_online AJAX action). | 8.8 | More Details |
| CVE-2023-28634 | GLPI is a free asset and IT management software package. Starting in version 0.83 and prior to versions 9.5.13 and 10.0.7, a user who has the Technician profile could see and generate a Personal token for a Super-Admin. Using such token it is possible to negotiate a GLPI session and hijack the Super-Admin account, resulting in a Privilege Escalation. Versions 9.5.13 and 10.0.7 contain a patch for this issue. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-21727 | Remote Procedure Call Runtime Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2020-19803 | Cross Site Request Forgery vulnerability found in Milken DoyoCMS v.2.3 allows a remote attacker to execute arbitrary code via the background system settings. | 8.8 | More Details |
| CVE-2022-43955 | An improper neutralization of input during web page generation [CWE-79] in the FortiWeb web interface 7.0.0 through 7.0.3, 6.3.0 through 6.3.21, 6.4 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow an unauthenticated and remote attacker to perform a reflected cross site scripting attack (XSS) via injecting malicious payload in log entries used to build report. | 8.8 | More Details |
| CVE-2022-41330 | An improper neutralization of input during web page generation vulnerability ('Cross-site Scripting') [CWE-79] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9, version 6.4.0 through 6.4.11 and before 6.2.12 and FortiProxy version 7.2.0 through 7.2.1 and before 7.0.7 allows an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests. | 8.8 | More Details |
| CVE-2023-26817 | codefever before 2023.2.7-commit-b1c2e7f was discovered to contain a remote code execution (RCE) vulnerability via the component /controllers/api/user.php. | 8.8 | More Details |
| CVE-2020-36077 | SQL injection vulnerability found in Tailor Mangement System v.1 allows a remote attacker to execute arbitrary code via the customer parameter of the orderadd.php file | 8.8 | More Details |
| CVE-2023-26860 | SQL injection vulnerability found in PrestaShop lgbudget v.1.0.3 and before allow a remote attacker to gain privileges via the LgBudgetBudgetModuleFrontController::displayAjaxGenerateBudget component. | 8.8 | More Details |
| CVE-2023-1406 | The JetEngine WordPress plugin before 3.1.3.1 includes uploaded files without adequately ensuring that they are not executable, leading to a remote code execution vulnerability. | 8.8 | More Details |
| CVE-2023-1381 | The WP Meta SEO WordPress plugin before 4.5.5 does not validate image file paths before attempting to manipulate the image files, leading to a PHAR deserialization vulnerability. Furthermore, the plugin contains a gadget chain which may be used in certain configurations to achieve remote code execution. | 8.8 | More Details |
| CVE-2023-28205 | A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.4.1, iOS 15.7.5 and iPadOS 15.7.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-29008 | The SvelteKit framework offers developers an option to create simple REST APIs. This is done by defining a `+server.js` file, containing endpoint handlers for different HTTP methods. SvelteKit provides out-of-the-box cross-site request forgery (CSRF) protection to its users. The protection is implemented at `kit/src/runtime/server/respond.js`. While the implementation does a sufficient job of mitigating common CSRF attacks, the protection can be bypassed in versions prior to 1.15.2 by simply specifying an upper-cased `Content-Type` header value. The browser will not send uppercase characters, but this check does not block all expected CORS requests. If abused, this issue will allow malicious requests to be submitted from third-party domains, which can allow execution of operations within the context of the victim's session, and in extreme scenarios can lead to unauthorized access to users' accounts. This may lead to all POST operations requiring authentication being allowed in the following cases: If the target site sets `SameSite=None` on its auth cookie and the user visits a malicious site in a Chromium-based browser; if the target site doesn't set the `SameSite` attribute explicitly and the user visits a malicious site with Firefox/Safari with tracking protections turned off; and/or if the user is visiting a malicious site with a very outdated browser. SvelteKit 1.15.2 contains a patch for this issue. It is also recommended to explicitly set `SameSite` to a value other than `None` on authentication cookies especially if the upgrade cannot be done in a timely manner. | 8.8 | More Details |
| CVE-2020-36074 | SQL injection vulnerability found in Tailor Mangement System v.1 allows a remote attacker to execute arbitrary code via the title parameter. | 8.8 | More Details |
| CVE-2020-36073 | SQL injection vulnerability found in Tailor Management System v.1 allows a remote attacker to execute arbitrary code via the detail parameter of the document.php page. | 8.8 | More Details |
| CVE-2020-36072 | SQL injection vulnerability found in Tailor Management System v.1 allows a remote attacker to execute arbitrary code via the id parameter. | 8.8 | More Details |
| CVE-2020-36071 | SQL injection vulnerability found in Tailor Management System v.1 allows a remote authenticated attacker to execute arbitrary code via the customer parameter of the email.php page. | 8.8 | More Details |
| CVE-2023-26122 | All versions of the package safe-eval are vulnerable to Sandbox Bypass due to improper input sanitization. The vulnerability is derived from prototype pollution exploitation. Exploiting this vulnerability might result in remote code execution ("RCE"). **Vulnerable functions:** __defineGetter__, stack(), toLocaleString(), propertyIsEnumerable.call(), valueOf(). | 8.8 | More Details |
| CVE-2023-27917 | OS command injection vulnerability in CONPROSYS IoT Gateway products allows a remote authenticated attacker who can access Network Maintenance page to execute arbitrary OS commands with a root privilege. The affected products and versions are as follows: M2M Gateway with the firmware Ver.3.7.10 and earlier (CPS-MG341-ADSC1-111, CPS-MG341-ADSC1-931, CPS-MG341G-ADSC1-111, CPS-MG341G-ADSC1-930, and CPS-MG341G5-ADSC1-931), M2M Controller Integrated Type with firmware Ver.3.7.6 and earlier versions (CPS-MC341-ADSC1-111, CPS-MC341-ADSC1-931, CPS-MC341-ADSC2-111, CPS-MC341G-ADSC1-110, CPS-MC341Q-ADSC1-111, CPS-MC341-DS1-111, CPS-MC341-DS11-111, CPS-MC341-DS2-911, and CPS-MC341-A1-111), and M2M Controller Configurable Type with firmware Ver.3.8.8 and earlier versions (CPS-MCS341-DS1-111, CPS-MCS341-DS1-131, CPS-MCS341G-DS1-130, CPS-MCS341G5-DS1-130, and CPS-MCS341Q-DS1-131). | 8.8 | More Details |
| CVE-2023-29421 | An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is an out-of-bounds write in bz3_decode_block. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1976 | Password Aging with Long Expiration in GitHub repository answerdev/answer prior to 1.0.6. | 8.8 | More Details |
| CVE-2023-28062 | Dell PPDM versions 19.12, 19.11 and 19.10, contain an improper access control vulnerability. A remote authenticated malicious user with low privileges could potentially exploit this vulnerability to bypass intended access restrictions and perform unauthorized actions. | 8.8 | More Details |
| CVE-2022-31888 | Session Fixation vulnerability in in function login in class.auth.php in osTicket through 1.16.2. | 8.8 | More Details |
| CVE-2023-28240 | Windows Network Load Balancing Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2022-27487 | A improper privilege management in Fortinet FortiSandbox version 4.2.0 through 4.2.2, 4.0.0 through 4.0.2 and before 3.2.3 and FortiDeceptor version 4.1.0, 4.0.0 through 4.0.2 and before 3.3.3 allows a remote authenticated attacker to perform unauthorized API calls via crafted HTTP or HTTPS requests. | 8.8 | More Details |
| CVE-2023-28297 | Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability | 8.8 | More Details |
| CVE-2023-28275 | Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability | 8.8 | More Details |
| CVE-2023-29186 | In SAP NetWeaver (BI CONT ADDON) - versions 707, 737, 747, 757, an attacker can exploit a directory traversal flaw in a report to upload and overwrite files on the SAP server. Data cannot be read but if a remote attacker has sufficient (administrative) privileges then potentially critical OS files can be overwritten making the system unavailable. | 8.7 | More Details |
| CVE-2023-28206 | An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1, iOS 15.7.5 and iPadOS 15.7.5, macOS Big Sur 11.7.6. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. | 8.6 | More Details |
| CVE-2023-22615 | An issue was discovered in IhisiSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. IHISI subfunction execution may corrupt SMRAM. An attacker can pass an address in the RCX save state register that overlaps SMRAM, thereby coercing an IHISI subfunction handler to overwrite private SMRAM. | 8.4 | More Details |
| CVE-2023-28291 | Raw Image Extension Remote Code Execution Vulnerability | 8.4 | More Details |
| CVE-2023-1668 | A flaw was found in openvswitch (OVS). When processing an IP packet with protocol 0, OVS will install the datapath flow without the action modifying the IP header. This issue results (for both kernel and userspace datapath) in installing a datapath flow matching all IP protocols (nw_proto is wildcarded) for this flow, but with an incorrect action, possibly causing incorrect handling of other IP packets with a != 0 IP protocol that matches this dp flow. | 8.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28288 | Microsoft SharePoint Server Spoofing Vulnerability | 8.1 | More Details |
| CVE-2023-28632 | GLPI is a free asset and IT management software package. Starting in version 0.83 and prior to versions 9.5.13 and 10.0.7, an authenticated user can modify emails of any user, and can therefore takeover another user account through the "forgotten password" feature. By modifying emails, the user can also receive sensitive data through GLPI notifications. Versions 9.5.13 and 10.0.7 contain a patch for this issue. As a workaround, account takeover can be prevented by deactivating all notifications related to `Forgotten password?` event. However, it will not prevent unauthorized modification of any user emails. | 8.1 | More Details |
| CVE-2023-25409 | Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. Restricted users have access to other users outlets. | 8.1 | More Details |
| CVE-2023-26067 | Certain Lexmark devices through 2023-02-19 mishandle Input Validation (issue 1 of 4). | 8.1 | More Details |
| CVE-2023-28219 | Layer 2 Tunneling Protocol Remote Code Execution Vulnerability | 8.1 | More Details |
| CVE-2023-28220 | Layer 2 Tunneling Protocol Remote Code Execution Vulnerability | 8.1 | More Details |
| CVE-2023-28268 | Netlogon RPC Elevation of Privilege Vulnerability | 8.1 | More Details |
| CVE-2023-24544 | Improper access control vulnerability in Buffalo network devices allows a network-adjacent attacker to obtain specific files of the product. As a result, the product settings may be altered. The affected products and versions are as follows: BS-GSL2024 firmware Ver. 1.10-0.03 and earlier, BS-GSL2016P firmware Ver. 1.10-0.03 and earlier, BS-GSL2016 firmware Ver. 1.10-0.03 and earlier, BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier | 8.1 | More Details |
| CVE-2023-28244 | Windows Kerberos Elevation of Privilege Vulnerability | 8.1 | More Details |
| CVE-2023-28272 | Windows Kernel Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-29053 | A vulnerability has been identified in JT Open (All versions < V11.3.2.0), JT Utilities (All versions < V13.3.0.0). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28285 | Microsoft Office Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-28262 | Visual Studio Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2022-45115 | A buffer overflow vulnerability exists in the Attribute Arena functionality of Ichitaro 2022 1.0.1.57600. A specially crafted document can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability. | 7.8 | More Details |
| CVE-2022-43664 | A use-after-free vulnerability exists within the way Ichitaro Word Processor 2022, version 1.0.1.57600, processes protected documents. A specially crafted document can trigger reuse of freed memory, which can lead to further memory corruption and potentially result in arbitrary code execution. An attacker can provide a malicious document to trigger this vulnerability. | 7.8 | More Details |
| CVE-2022-40679 | An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC 5.x all versions, 6.0 all versions, 6.1 all versions, 6.2.0 through 6.2.4, 7.0.0 through 7.0.3, 7.1.0; FortiDDoS 4.x all versions, 5.0 all versions, 5.1 all versions, 5.2 all versions, 5.3 all versions, 5.4 all versions, 5.5 all versions, 5.6 all versions and FortiDDoS-F 6.4.0, 6.3.0 through 6.3.3, 6.2.0 through 6.2.2, 6.1.0 through 6.1.4 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. | 7.8 | More Details |
| CVE-2022-40682 | A incorrect authorization in Fortinet FortiClient (Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9, 6.2.0 - 6.2.9 and 6.0.0 - 6.0.10 allows an attacker to execute unauthorized code or commands via sending a crafted request to a specific named pipe. | 7.8 | More Details |
| CVE-2022-42470 | A relative path traversal vulnerability in Fortinet FortiClient (Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9, 6.2.0 - 6.2.9 and 6.0.0 - 6.0.10 allows an attacker to execute unauthorized code or commands via sending a crafted request to a specific named pipe. | 7.8 | More Details |
| CVE-2023-24912 | Windows Graphics Component Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-28292 | Raw Image Extension Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-25755 | Screen Creator Advance 2 Ver.0.1.1.4 Build01A and earlier is vulnerable to improper restriction of operations within the bounds of a memory buffer (CWE-119) due to improper check of its data size when processing a project file. If a user of Screen Creator Advance 2 opens a specially crafted project file, information may be disclosed and/or arbitrary code may be executed. | 7.8 | More Details |
| CVE-2023-28274 | Windows Win32k Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-24893 | Visual Studio Code Remote Code Execution Vulnerability | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-46878 | An issue was discovered in Treasure Data Fluent Bit 1.7.1, erroneous parsing in flb_pack_msgpack_to_json_format leads to type confusion bug that interprets whatever is on the stack as msgpack maps and arrays, leading to use-after-free. This can be used by an attacker to craft a specially craft file and trick the victim opening it using the affect software, triggering use-after-free and execute arbitrary code on the target system. | 7.8 | More Details |
| CVE-2021-46879 | An issue was discovered in Treasure Data Fluent Bit 1.7.1, a wrong variable is used to get the msgpack data resulting in a heap overflow in flb_msgpack_gelf_value_ext. An attacker can craft a malicious file and tick the victim to open the file with the software, triggering a heap overflow and execute arbitrary code on the target system. | 7.8 | More Details |
| CVE-2023-28296 | Visual Studio Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-22429 | Android App 'Wolt Delivery: Food and more' version 4.27.2 and earlier uses hard-coded credentials (API key for an external service), which may allow a local attacker to obtain the hard-coded API key via reverse-engineering the application binary. | 7.8 | More Details |
| CVE-2023-28293 | Windows Kernel Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-23375 | Microsoft ODBC and OLE DB Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-26593 | CENTUM series provided by Yokogawa Electric Corporation are vulnerable to cleartext storage of sensitive information. If an attacker who can login or access the computer where the affected product is installed tampers the password file stored in the computer, the user privilege which CENTUM managed may be escalated. As a result, the control system may be operated with the escalated user privilege. To exploit this vulnerability, the following prerequisites must be met: (1)An attacker has obtained user credentials where the affected product is installed, (2)CENTUM Authentication Mode is used for user authentication when CENTUM VP is used. The affected products and versions are as follows: CENTUM CS 1000, CENTUM CS 3000 (Including CENTUM CS 3000 Entry Class) R2.01.00 to R3.09.50, CENTUM VP (Including CENTUM VP Entry Class) R4.01.00 to R4.03.00, R5.01.00 to R5.04.20, and R6.01.00 and later, B/M9000 CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R7.04.51 and R8.01.01 and later | 7.8 | More Details |
| CVE-2023-28304 | Microsoft ODBC and OLE DB Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-28246 | Windows Registry Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-28248 | Windows Kernel Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2022-42858 | A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.1. An app may be able to execute arbitrary code with kernel privileges | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28051 | Dell Power Manager, versions 3.10 and prior, contains an Improper Access Control vulnerability. A low-privileged attacker could potentially exploit this vulnerability to elevate privileges on the system. | 7.8 | More Details |
| CVE-2023-28237 | Windows Kernel Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-28236 | Windows Kernel Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-28252 | Windows Common Log File System Driver Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-28225 | Windows NTLM Elevation of Privilege Vulnerability | 7.8 | More Details |
| CVE-2023-28311 | Microsoft Word Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-26986 | An issue in China Mobile OA Mailbox PC v2.9.23 allows remote attackers to execute arbitrary commands on a victim host via user interaction with a crafted EML file sent to their OA mailbox. | 7.8 | More Details |
| CVE-2023-28260 | .NET DLL Hijacking Remote Code Execution Vulnerability | 7.8 | More Details |
| CVE-2023-20655 | In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. | 7.8 | More Details |
| CVE-2023-26495 | An issue was discovered in Open Design Alliance Drawings SDK before 2024.1. A crafted DWG file can force the SDK to reuse an object that has been freed. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code. | 7.8 | More Details |
| CVE-2023-26466 | A user with non-Admin access can change a configuration file on the client to modify the Server URL. | 7.8 | More Details |
| CVE-2023-23761 | An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to modify other users' secret gists by authenticating through an SSH certificate authority. To do so, a user had to know the secret gist's URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. | 7.7 | More Details |
| CVE-2023-28309 | Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability | 7.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-46716 | A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2. Private Relay functionality did not match system settings | 7.5 | More Details |
| CVE-2023-26917 | libyang from v2.0.164 to v2.1.30 was discovered to contain a NULL pointer dereference via the function lysp_stmt_validate_value at lys_parse_mem.c. | 7.5 | More Details |
| CVE-2023-28766 | A vulnerability has been identified in SIPROTEC 5 6MD85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 6MD86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 6MD89 (CP300) (All versions >= V7.80 < V9.64), SIPROTEC 5 6MU85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7KE85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions < V9.40), SIPROTEC 5 7SA86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SA87 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions < V9.40), SIPROTEC 5 7SD86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SD87 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SJ81 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ81 (CP150) (All versions < V9.40), SIPROTEC 5 7SJ82 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ82 (CP150) (All versions < V9.40), SIPROTEC 5 7SJ85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SJ86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SK82 (CP100) (All versions < V8.89), SIPROTEC 5 7SK82 (CP150) (All versions < V9.40), SIPROTEC 5 7SK85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions < V9.40), SIPROTEC 5 7SL86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SL87 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SS85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7ST85 (CP300) (All versions >= V7.80 < V9.64), SIPROTEC 5 7ST86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7SX82 (CP150) (All versions < V9.40), SIPROTEC 5 7SX85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7UM85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions < V9.40), SIPROTEC 5 7UT85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7UT86 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7UT87 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7VE85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7VK87 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 7VU85 (CP300) (All versions >= V7.80 < V9.40), SIPROTEC 5 Communication Module ETH-BA-2EL (All versions < V9.40 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (All versions < V9.40 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BD-2FO (All versions < V9.40), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V9.40). Affected devices lack proper validation of http request parameters of the hosted web service. An unauthenticated remote attacker could send specially crafted packets that could cause denial of service condition of the target device. | 7.5 | More Details |
| CVE-2023-28300 | Azure Service Connector Security Feature Bypass Vulnerability | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-24536 | Multipart form parsing can consume large amounts of CPU and memory when processing form inputs containing very large numbers of parts. This stems from several causes: 1. mime/multipart.Reader.ReadForm limits the total memory a parsed multipart form can consume. ReadForm can undercount the amount of memory consumed, leading it to accept larger inputs than intended. 2. Limiting total memory does not account for increased pressure on the garbage collector from large numbers of small allocations in forms with many parts. 3. ReadForm can allocate a large number of short-lived buffers, further increasing pressure on the garbage collector. The combination of these factors can permit an attacker to cause an program that parses multipart forms to consume large amounts of CPU and memory, potentially resulting in a denial of service. This affects programs that use mime/multipart.Reader.ReadForm, as well as form parsing in the net/http package with the Request methods FormFile, FormValue, ParseMultipartForm, and PostFormValue. With fix, ReadForm now does a better job of estimating the memory consumption of parsed forms, and performs many fewer short-lived allocations. In addition, the fixed mime/multipart.Reader imposes the following limits on the size of parsed forms: 1. Forms parsed with ReadForm may contain no more than 1000 parts. This limit may be adjusted with the environment variable GODEBUG=multipartmaxparts=. 2. Form parts parsed with NextPart and NextRawPart may contain no more than 10,000 header fields. In addition, forms parsed with ReadForm may contain no more than 10,000 header fields across all parts. This limit may be adjusted with the environment variable GODEBUG=multipartmaxheaders=. | 7.5 | More Details |
| CVE-2023-26820 | siteproxy v1.0 was discovered to contain a path traversal vulnerability via the component index.js. | 7.5 | More Details |
| CVE-2023-28302 | Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-27179 | GDidees CMS v3.9.1 and lower was discovered to contain an arbitrary file download vulenrability via the filename parameter at /_admin/imgdownload.php. | 7.5 | More Details |
| CVE-2023-27727 | Nginx NJS v0.7.10 was discovered to contain a segmentation violation via the function njs_function_frame at src/njs_function.h. | 7.5 | More Details |
| CVE-2023-26964 | An issue was discovered in hyper v0.13.7. h2-0.2.4 Stream stacking occurs when the H2 component processes HTTP2 RST_STREAM frames. As a result, the memory and CPU usage are high which can lead to a Denial of Service (DoS). | 7.5 | More Details |
| CVE-2023-28710 | Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Spark Provider.This issue affects Apache Airflow Spark Provider: before 4.0.1. | 7.5 | More Details |
| CVE-2023-28707 | Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Drill Provider.This issue affects Apache Airflow Drill Provider: before 2.3.2. | 7.5 | More Details |
| CVE-2023-27180 | GDidees CMS v3.9.1 was discovered to contain a source code disclosure vulnerability by the backup feature which is accessible via /_admin/backup.php. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-43768 | A vulnerability has been identified in SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.3), SIMATIC CP 443-1 (6GK7443-1EX30-0XE0) (All versions < V3.3), SIMATIC CP 443-1 (6GK7443-1EX30-0XE1) (All versions < V3.3), SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0) (All versions < V3.3), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.3), SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0) (All versions < V3.4.29), SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0) (All versions < V3.3), SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0) (All versions < V3.3), SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0) (All versions < V3.4.29), SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0) (All versions < V3.4.29), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.3.6), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.3.6). The webserver of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of the webserver of the affected product. | 7.5 | More Details |
| CVE-2023-27728 | Nginx NJS v0.7.10 was discovered to contain a segmentation violation via the function njs_dump_is_recursive at src/njs_vmcode.c. | 7.5 | More Details |
| CVE-2023-27191 | An issue found in DUALSPACE Super Secuirty v.2.3.7 allows an attacker to cause a denial of service via the SharedPreference files. | 7.5 | More Details |
| CVE-2022-43716 | A vulnerability has been identified in SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.3), SIMATIC CP 443-1 (6GK7443-1EX30-0XE0) (All versions < V3.3), SIMATIC CP 443-1 (6GK7443-1EX30-0XE1) (All versions < V3.3), SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0) (All versions < V3.3), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.3), SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0) (All versions < V3.4.29), SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0) (All versions < V3.3), SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0) (All versions < V3.3), SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0) (All versions < V3.4.29), SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0) (All versions < V3.4.29), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.3.6), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.3.6). The webserver of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation which leads to a restart of the webserver of the affected product. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27729 | Nginx NJS v0.7.10 was discovered to contain an illegal memcpy via the function njs_vmcode_return at src/njs_vmcode.c. | 7.5 | More Details |
| CVE-2023-27730 | Nginx NJS v0.7.10 was discovered to contain a segmentation violation via the function njs_lvlhsh_find at src/njs_lvlhsh.c. | 7.5 | More Details |
| CVE-2023-26588 | Use of hard-coded credentials vulnerability in Buffalo network devices allows an attacker to access the debug function of the product. The affected products and versions are as follows: BS-GSL2024 firmware Ver. 1.10-0.03 and earlier, BS-GSL2016P firmware Ver. 1.10-0.03 and earlier, BS-GSL2016 firmware Ver. 1.10-0.03 and earlier, BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier | 7.5 | More Details |
| CVE-2023-24534 | HTTP and MIME header parsing can allocate large amounts of memory, even when parsing small inputs, potentially leading to a denial of service. Certain unusual patterns of input data can cause the common function used to parse HTTP and MIME headers to allocate substantially more memory than required to hold the parsed headers. An attacker can exploit this behavior to cause an HTTP server to allocate large amounts of memory from a small request, potentially leading to memory exhaustion and a denial of service. With fix, header parsing now correctly allocates only the memory required to hold parsed headers. | 7.5 | More Details |
| CVE-2023-24537 | Calling any of the Parse functions on Go source code which contains //line directives with very large line numbers can cause an infinite loop due to integer overflow. | 7.5 | More Details |
| CVE-2021-45985 | In Lua 5.4.3, an erroneous finalizer called during a tail call leads to a heap-based buffer over-read. | 7.5 | More Details |
| CVE-2023-26774 | An issue found in Sales Tracker Management System v.1.0 allows a remote attacker to access sensitive information via sales.php component of the admin/reports endpoint. | 7.5 | More Details |
| CVE-2020-19678 | Directory Traversal vulnerability found in Pfsense v.2.1.3 and Pfsense Suricata v.1.4.6 pkg v.1.0.1 allows a remote attacker to obtain sensitive information via the file parameter to suricata/suricata_logs_browser.php. | 7.5 | More Details |
| CVE-2023-26121 | All versions of the package safe-eval are vulnerable to Prototype Pollution via the safeEval function, due to improper sanitization of its parameter content. | 7.5 | More Details |
| CVE-2023-29005 | Flask-AppBuilder versions before 4.3.0 lack rate limiting which can allow an attacker to brute-force user credentials. Version 4.3.0 includes the ability to enable rate limiting using `AUTH_RATE_LIMITED = True`, `RATELIMIT_ENABLED = True`, and setting an `AUTH_RATE_LIMIT`. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-43767 | A vulnerability has been identified in SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-1 IEC (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0) (All versions < V3.4.29), SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.3), SIMATIC CP 443-1 (6GK7443-1EX30-0XE0) (All versions < V3.3), SIMATIC CP 443-1 (6GK7443-1EX30-0XE1) (All versions < V3.3), SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0) (All versions < V3.3), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.3), SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0) (All versions < V3.4.29), SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0) (All versions < V3.3), SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0) (All versions < V3.3), SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0) (All versions < V3.4.29), SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0) (All versions < V3.4.29), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.3.6), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.3.6). The webserver of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of the webserver of the affected product. | 7.5 | More Details |
| CVE-2023-28217 | Windows Network Address Translation (NAT) Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-22642 | An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. | 7.5 | More Details |
| CVE-2023-28227 | Windows Bluetooth Driver Remote Code Execution Vulnerability | 7.5 | More Details |
| CVE-2023-24860 | Microsoft Defender Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-28247 | Windows Network File System Information Disclosure Vulnerability | 7.5 | More Details |
| CVE-2023-28241 | Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-28238 | Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability | 7.5 | More Details |
| CVE-2023-28232 | Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-21769 | Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-28342 | Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. | 7.5 | More Details |
| CVE-2023-24931 | Windows Secure Channel Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-28233 | Windows Secure Channel Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2023-28234 | Windows Secure Channel Denial of Service Vulnerability | 7.5 | More Details |
| CVE-2022-43946 | Multiple vulnerabilities including an incorrect permission assignment for critical resource [CWE-732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. | 7.5 | More Details |
| CVE-2023-25413 | Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. The device allows unauthenticated access to Telnet and SNMP credentials. | 7.5 | More Details |
| CVE-2023-1941 | A vulnerability, which was classified as critical, has been found in SourceCodester Simple and Beautiful Shopping Cart System 1.0. This issue affects some unknown processing of the file login.php. The manipulation of the argument username/password 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-225317 was assigned to this vulnerability. | 7.3 | More Details |
| CVE-2022-38604 | Wacom Driver 6.3.46-1 for Windows and lower was discovered to contain an arbitrary file deletion vulnerability. | 7.3 | More Details |
| CVE-2022-4940 | The WCFM Membership plugin for WordPress is vulnerable to unauthorized modification and access of data in versions up to, and including, 2.10.0 due to missing capability checks on various AJAX actions. This makes it possible for unauthenticated attackers to perform a wide variety of actions such as modifying membership details, changing renewal information, controlling membership approvals, and more. | 7.3 | More Details |
| CVE-2023-1955 | A vulnerability classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected is an unknown function of the file login.php of the component User Registration. The manipulation of the argument email 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-225342 is the identifier assigned to this vulnerability. | 7.3 | More Details |
| CVE-2023-22282 | WAB-MAT Ver.5.0.0.8 and earlier starts another program with an unquoted file path. Since a registered Windows service path contains spaces and are unquoted, if a malicious executable is placed on a certain path, the executable may be executed with the privilege of the Windows service. | 7.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1964 | A vulnerability classified as critical has been found in PHPGurukul Bank Locker Management System 1.0. Affected is an unknown function of the file recovery.php of the component Password Reset. The manipulation of the argument uname/mobile leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225360. | 7.3 | More Details |
| CVE-2023-1886 | Authentication Bypass by Capture-replay in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 7.3 | More Details |
| CVE-2023-25950 | HTTP request/response smuggling vulnerability in HAProxy version 2.7.0, and 2.6.1 to 2.6.7 allows a remote attacker to alter a legitimate user's request. As a result, the attacker may obtain sensitive information or cause a denial-of-service (DoS) condition. | 7.3 | More Details |
| CVE-2023-23384 | Microsoft SQL Server Remote Code Execution Vulnerability | 7.3 | More Details |
| CVE-2023-1962 | A vulnerability classified as critical was found in SourceCodester Best Online News Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225361 was assigned to this vulnerability. | 7.3 | More Details |
| CVE-2023-26293 | A vulnerability has been identified in Totally Integrated Automation Portal (TIA Portal) V15 (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions < V16 Update 7), Totally Integrated Automation Portal (TIA Portal) V17 (All versions < V17 Update 6), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 1). Affected products contain a path traversal vulnerability that could allow the creation or overwrite of arbitrary files in the engineering system. If the user is tricked to open a malicious PC system configuration file, an attacker could exploit this vulnerability to achieve arbitrary code execution. | 7.3 | More Details |
| CVE-2023-22635 | A download of code without Integrity check vulnerability [CWE-494] in FortiClientMac version 7.0.0 through 7.0.7, 6.4 all versions, 6.2 all versions, 6.0 all versions, 5.6 all versions, 5.4 all versions, 5.2 all versions, 5.0 all versions and 4.0 all versions may allow a local attacker to escalate their privileges via modifying the installer upon upgrade. | 7.3 | More Details |
| CVE-2023-1912 | The Limit Login Attempts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its lock logging feature in versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the plugin's settings page. This only works when the plugin prioritizes use of the X-FORWARDED-FOR header, which can be configured in its settings. | 7.2 | More Details |
| CVE-2023-20117 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as the root user on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27995 | A improper neutralization of special elements used in a template engine vulnerability in Fortinet FortiSOAR 7.3.0 through 7.3.1 allows an authenticated, remote attacker to execute arbitrary code via a crafted payload. | 7.2 | More Details |
| CVE-2023-26919 | delight-nashorn-sandbox 0.2.4 and 0.2.5 is vulnerable to sandbox escape. When allowExitFunctions is set to false, the loadWithNewGlobal function can be used to invoke the exit and quit methods to exit the Java process. | 7.2 | More Details |
| CVE-2023-0670 | Ulearn version a5a7ca20de859051ea0470542844980a66dfc05d allows an attacker with administrator permissions to obtain remote code execution on the server through the image upload functionality. This occurs because the application does not validate that the uploaded image is actually an image. | 7.2 | More Details |
| CVE-2023-25407 | Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. Restricted users have read access to administrator credentials. | 7.2 | More Details |
| CVE-2023-27389 | Inadequate encryption strength vulnerability in CONPROSYS IoT Gateway products allows a remote authenticated attacker with an administrative privilege to apply a specially crafted Firmware update file, alter the information, cause a denial-of-service (DoS) condition, and/or execute arbitrary code. The affected products and versions are as follows: M2M Gateway with the firmware Ver.3.7.10 and earlier (CPS-MG341-ADSC1-111, CPS-MG341-ADSC1-931, CPS-MG341G-ADSC1-111, CPS-MG341G-ADSC1-930, and CPS-MG341G5-ADSC1-931), M2M Controller Integrated Type with firmware Ver.3.7.6 and earlier versions (CPS-MC341-ADSC1-111, CPS-MC341-ADSC1-931, CPS-MC341-ADSC2-111, CPS-MC341G-ADSC1-110, CPS-MC341Q-ADSC1-111, CPS-MC341-DS1-111, CPS-MC341-DS11-111, CPS-MC341-DS2-911, and CPS-MC341-A1-111), and M2M Controller Configurable Type with firmware Ver.3.8.8 and earlier versions (CPS-MCS341-DS1-111, CPS-MCS341-DS1-131, CPS-MCS341G-DS1-130, CPS-MCS341G5-DS1-130, and CPS-MCS341Q-DS1-131). | 7.2 | More Details |
| CVE-2023-26856 | Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter at /admin/ajax.php?action=login. | 7.2 | More Details |
| CVE-2023-1425 | The WordPress CRM, Email & Marketing Automation for WordPress | Award Winner — Groundhogg WordPress plugin before 2.7.9.4 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admins | 7.2 | More Details |
| CVE-2023-28254 | Windows DNS Server Remote Code Execution Vulnerability | 7.2 | More Details |
| CVE-2023-20128 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as the root user on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. | 7.2 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-26857 | An arbitrary file upload vulnerability in /admin/ajax.php?action=save_uploads of Dynamic Transaction Queuing System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. | 7.2 | More Details |
| CVE-2022-47338 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 7.1 | More Details |
| CVE-2023-29236 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Cththemes Outdoor theme <= 3.9.6 versions. | 7.1 | More Details |
| CVE-2023-25713 | Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Paypal Payments plugin <= 5.7.25 versions. | 7.1 | More Details |
| CVE-2023-1838 | A use-after-free flaw was found in vhost_net_set_backend in drivers/vhost/net.c in virtio network subcomponent in the Linux kernel due to a double fget. This flaw could allow a local attacker to crash the system, and could even lead to a kernel information leak problem. | 7.1 | More Details |
| CVE-2022-42477 | An improper input validation vulnerability [CWE-20] in FortiAnalyzer version 7.2.1 and below, version 7.0.6 and below, 6.4 all versions may allow an authenticated attacker to disclose file system information via custom dataset SQL queries. | 7.1 | More Details |
| CVE-2023-28993 | Unauth.  Reflected Cross-Site Scripting (XSS) vulnerability in Ignazio Scimone Albo Pretorio On Line plugin <= 4.6.1 versions. | 7.1 | More Details |
| CVE-2023-25020 | Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.1.1 versions. | 7.1 | More Details |
| CVE-2023-27876 | IBM TRIRIGA 4.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 249975. | 7.1 | More Details |
| CVE-2023-28789 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Cimatti Consulting WordPress Contact Forms by Cimatti plugin <= 1.5.4 versions. | 7.1 | More Details |
| CVE-2023-29388 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in impleCode Product Catalog Simple plugin <= 1.6.17 versions. | 7.1 | More Details |
| CVE-2023-29172 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PropertyHive plugin <= 1.5.46 versions. | 7.1 | More Details |
| CVE-2023-28222 | Windows Kernel Elevation of Privilege Vulnerability | 7.1 | More Details |
| CVE-2023-29171 | Unauth. Reflected Cross-site Scripting (XSS) vulnerability in Magic Post Thumbnail plugin <= 4.1.10 versions. | 7.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28792 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Continuous Image Carousel With Lightbox plugin <= 1.0.15 versions. | 7.1 | More Details |
| CVE-2023-23979 | Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Event Manager plugin <= 9.7.4 versions. | 7.1 | More Details |
| CVE-2023-28781 | Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Cimatti Consulting WordPress Contact Forms by Cimatti plugin <= 1.5.4 versions. | 7.1 | More Details |
| CVE-2023-28224 | Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability | 7.1 | More Details |
| CVE-2023-25041 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Cththemes Monolit theme <= 2.0.6 versions. | 7.1 | More Details |
| CVE-2023-28229 | Windows CNG Key Isolation Service Elevation of Privilege Vulnerability | 7.0 | More Details |
| CVE-2023-28218 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | 7.0 | More Details |
| CVE-2023-28221 | Windows Error Reporting Service Elevation of Privilege Vulnerability | 7.0 | More Details |
| CVE-2023-28216 | Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability | 7.0 | More Details |
| CVE-2023-1412 | An unprivileged (non-admin) user can exploit an Improper Access Control vulnerability in the Cloudflare WARP Client for Windows (<= 2022.12.582.0) to perform privileged operations with SYSTEM context by working with a combination of opportunistic locks (oplock) and symbolic links (which can both be created by an unprivileged user). After installing the Cloudflare WARP Client (admin privileges required), an MSI-Installer is placed under C:\Windows\Installer. The vulnerability lies in the repair function of this MSI. ImpactAn unprivileged (non-admin) user can exploit this vulnerability to perform privileged operations with SYSTEM context, including deleting arbitrary files and reading arbitrary file content. This can lead to a variety of attacks, including the manipulation of system files and privilege escalation. PatchesA new installer with a fix that addresses this vulnerability was released in version 2023.3.381.0. While the WARP Client itself is not vulnerable (only the installer), users are encouraged to upgrade to the latest version and delete any older installers present in their systems. | 7.0 | More Details |
| CVE-2023-24914 | Win32k Elevation of Privilege Vulnerability | 7.0 | More Details |
| CVE-2023-22291 | An invalid free vulnerability exists in the Frame stream parser functionality of Ichitaro 2022 1.0.1.57600. A specially crafted document can lead to an attempt to free a stack pointer, which causes memory corruption. An attacker can provide a malicious file to trigger this vulnerability. | 7.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0652 | Due to a hardlink created in the ProgramData folder during the repair process of the software, the installer (MSI) of WARP Client for Windows (<= 2022.12.582.0) allowed a malicious attacker to forge the destination of the hardlink and escalate privileges, overwriting SYSTEM protected files. As Cloudflare WARP client for Windows (up to version 2022.5.309.0) allowed creation of mount points from its ProgramData folder, during installation of the WARP client, it was possible to escalate privileges and overwrite SYSTEM protected files. | 7.0 | More Details |
| CVE-2023-28273 | Windows Clip Service Elevation of Privilege Vulnerability | 7.0 | More Details |
| CVE-2023-1989 | A use-after-free flaw was found in btsdio_remove in drivers\bluetooth\btsdio.c in the Linux Kernel. In this flaw, a call to btsdio_remove with an unfinished job, may cause a race problem leading to a UAF on hdev devices. | 7.0 | More Details |
| CVE-2023-25542 | Dell Trusted Device Agent, versions prior to 5.3.0, contain(s) an improper installation permissions vulnerability. An unauthenticated local attacker could potentially exploit this vulnerability, leading to escalated privileges. | 7.0 | More Details |
| CVE-2023-22660 | A heap-based buffer overflow vulnerability exists in the way Ichitaro version 2022 1.0.1.57600 processes certain LayoutBox stream record types. A specially crafted document can cause a buffer overflow, leading to memory corruption, which can result in arbitrary code execution.To trigger this vulnerability, the victim would need to open a malicious, attacker-created document. | 7.0 | More Details |
| CVE-2023-28235 | Windows Lock Screen Security Feature Bypass Vulnerability | 6.8 | More Details |
| CVE-2023-28270 | Windows Lock Screen Security Feature Bypass Vulnerability | 6.8 | More Details |
| CVE-2023-29389 | Toyota RAV4 2021 vehicles automatically trust messages from other ECUs on a CAN bus, which allows physically proximate attackers to drive a vehicle by accessing the control CAN bus after pulling the bumper away and reaching the headlight connector, and then sending forged "Key is validated" messages via CAN Injection, as exploited in the wild in (for example) July 2022. | 6.8 | More Details |
| CVE-2023-26458 | An information disclosure vulnerability exists in SAP Landscape Management - version 3.0, enterprise edition. It allows an authenticated SAP Landscape Management user to obtain privileged access to other systems making those other systems vulnerable to information disclosure and modification.The disclosed information is for Diagnostics Agent Connection via Java SCS Message Server of an SAP Solution Manager system and can only be accessed by authenticated SAP Landscape Management users, but they can escalate their privileges to the SAP Solution Manager system. | 6.8 | More Details |
| CVE-2023-20682 | In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. | 6.7 | More Details |
| CVE-2023-20681 | In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20680 | In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. | 6.7 | More Details |
| CVE-2023-20653 | In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. | 6.7 | More Details |
| CVE-2023-20661 | In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. | 6.7 | More Details |
| CVE-2023-20670 | In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. | 6.7 | More Details |
| CVE-2023-20652 | In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. | 6.7 | More Details |
| CVE-2023-20654 | In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. | 6.7 | More Details |
| CVE-2023-20656 | In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. | 6.7 | More Details |
| CVE-2023-20657 | In mtee, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. | 6.7 | More Details |
| CVE-2023-29187 | A Windows user with basic user authorization can exploit a DLL hijacking attack in SapSetup (Software Installation Program) - version 9.0, resulting in a privilege escalation running code as administrator of the very same Windows PC. A successful attack depends on various preconditions beyond the attackers control. | 6.7 | More Details |
| CVE-2023-20658 | In isp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07537393; Issue ID: ALPS07180396. | 6.7 | More Details |
| CVE-2023-20659 | In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. | 6.7 | More Details |
| CVE-2022-32599 | In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07460390. | 6.7 | More Details |
| CVE-2023-20662 | In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. | 6.7 | More Details |
| CVE-2023-20663 | In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-29054 | A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT PRO (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2IRT (All versions < V5.5.2), SCALANCE X202-2P IRT (All versions < V5.5.2), SCALANCE X202-2P IRT PRO (All versions < V5.5.2), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT (All versions < V5.5.2), SCALANCE X204IRT PRO (All versions < V5.5.2), SCALANCE XF201-3P IRT (All versions < V5.5.2), SCALANCE XF202-2P IRT (All versions < V5.5.2), SCALANCE XF204-2BA IRT (All versions < V5.5.2), SCALANCE XF204IRT (All versions < V5.5.2), SIPLUS NET SCALANCE X202-2P IRT (All versions < V5.5.2). The SSH server on affected devices is configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device. | 6.7 | More Details |
| CVE-2023-20664 | In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. | 6.7 | More Details |
| CVE-2022-43948 | A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb version 7.0.0 through 7.0.3, FortiADC version 7.1.0 through 7.1.1, FortiADC version 7.0.0 through 7.0.3, FortiADC 6.2 all versions, FortiADC 6.1 all versions, FortiADC 6.0 all versions, FortiADC 5.4 all versions, FortiADC 5.3 all versions, FortiADC 5.2 all versions, FortiADC 5.1 all versions allows attacker to execute unauthorized code or commands via specifically crafted arguments to existing commands. | 6.7 | More Details |
| CVE-2023-20666 | In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. | 6.7 | More Details |
| CVE-2023-28046 | Dell Display Manager, versions 2.1.0 and prior, contains an arbitrary file or folder deletion vulnerability during uninstallation A local low privilege attacker could potentially exploit this vulnerability, leading to the deletion of arbitrary files on the operating system with high privileges. | 6.6 | More Details |
| CVE-2023-28256 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-28278 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-28223 | Windows Domain Name Service Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-28255 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-28307 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-28306 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28308 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-28305 | Windows DNS Server Remote Code Execution Vulnerability | 6.6 | More Details |
| CVE-2023-24626 | socket.c in GNU Screen through 4.9.0, when installed setuid or setgid (the default on platforms such as Arch Linux and FreeBSD), allows local users to send a privileged SIGHUP signal to any PID, causing a denial of service or disruption of the target process. | 6.5 | More Details |
| CVE-2023-24883 | Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability | 6.5 | More Details |
| CVE-2023-1426 | The WP Tiles WordPress plugin through 1.1.2 does not ensure that posts to be displayed are not draft/private, allowing any authenticated users, such as subscriber to retrieve the titles of draft and privates posts for example. AN attacker could also retrieve the title of any other type of post. | 6.5 | More Details |
| CVE-2023-27620 | Auth. (contributor+) Stored Cross-site Scripting (XSS) vulnerability in RoboSoft Photo Gallery, Images, Slider in Rbs Image Gallery plugin <= 3.2.12 versions. | 6.5 | More Details |
| CVE-2023-1975 | Insertion of Sensitive Information Into Sent Data in GitHub repository answerdev/answer prior to 1.0.8. | 6.5 | More Details |
| CVE-2023-1974 | Exposure of Sensitive Information Through Metadata in GitHub repository answerdev/answer prior to 1.0.8. | 6.5 | More Details |
| CVE-2023-1980 | Two factor authentication bypass on login in Devolutions Remote Desktop Manager 2022.3.35 and earlier allow user to cancel the two factor authentication via the application user interface and open entries. | 6.5 | More Details |
| CVE-2023-27520 | Cross-site request forgery (CSRF) vulnerability in SEIKO EPSON printers/network interface Web Config allows a remote unauthenticated attacker to hijack the authentication and perform unintended operations by having a logged-in user view a malicious page. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers/network interface via a web browser. According to SEIKO EPSON CORPORATION, it is also called as Remote Manager in some products. Web Config is pre-installed in some printers/network interface provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. | 6.5 | More Details |
| CVE-2023-30456 | An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4. | 6.5 | More Details |
| CVE-2023-28312 | Azure Machine Learning Information Disclosure Vulnerability | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-28763 | SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. | 6.5 | More Details |
| CVE-2023-28761 | In SAP NetWeaver Enterprise Portal - version 7.50, an unauthenticated attacker can attach to an open interface and make use of an open API to access a service which will enable them to access or modify server settings and data, leading to limited impact on confidentiality and integrity. | 6.5 | More Details |
| CVE-2023-28340 | Zoho ManageEngine Applications Manager through 16320 allows the admin user to conduct an XXE attack. | 6.5 | More Details |
| CVE-2023-28267 | Remote Desktop Protocol Client Information Disclosure Vulnerability | 6.5 | More Details |
| CVE-2022-27485 | A improper neutralization of special elements used in an sql command ('sql injection') vulnerability [CWE-89] in Fortinet FortiSandbox version 4.2.0, 4.0.0 through 4.0.2, 3.2.0 through 3.2.3, 3.1.x and 3.0.x allows a remote and authenticated attacker with read permission to retrieve arbitrary files from the underlying Linux system via a crafted HTTP request. | 6.5 | More Details |
| CVE-2023-28093 | A user with a compromised configuration can start an unsigned binary as a service. | 6.5 | More Details |
| CVE-2023-23762 | An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff. To do so, an attacker would need write access to the repository and be able to correctly guess the target branch before it’s created by the code maintainer. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. | 6.5 | More Details |
| CVE-2023-1801 | The SMB protocol decoder in tcpdump version 4.99.3 can perform an out-of-bounds write when decoding a crafted network packet. | 6.5 | More Details |
| CVE-2022-3695 | Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.3.0.0, 9.2.0.4 and 8.3.0.27 allow a malicious URL to inject content into a dashboard when the CDE plugin is present. | 6.5 | More Details |
| CVE-2023-0382 | User-controlled operations could have allowed Denial of Service in M-Files Server before 23.4.12528.1 due to uncontrolled memory consumption. | 6.5 | More Details |
| CVE-2023-0959 | Bhima version 1.27.0 allows a remote attacker to update the privileges of any account registered in the application via a malicious link sent to an administrator. This is possible because the application is vulnerable to CSRF. | 6.5 | More Details |
| CVE-2023-24003 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Timersys WP Popups – WordPress Popup plugin <= 2.1.4.8 versions. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20124 | A vulnerability in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. This vulnerability is due to improper validation of user input within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface. A successful exploit could allow the attacker to gain root-level privileges and access unauthorized data. To exploit this vulnerability, an attacker would need to have valid administrative credentials on the affected device. Cisco has not released software updates that address this vulnerability. | 6.5 | More Details |
| CVE-2023-20127 | Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. | 6.5 | More Details |
| CVE-2023-20129 | Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. | 6.5 | More Details |
| CVE-2023-20130 | Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. | 6.5 | More Details |
| CVE-2023-20131 | Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. | 6.5 | More Details |
| CVE-2023-25061 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.1.1 versions. | 6.5 | More Details |
| CVE-2023-28855 | Fields is a GLPI plugin that allows users to add custom fields on GLPI items forms. Prior to versions 1.13.1 and 1.20.4, lack of access control check allows any authenticated user to write data to any fields container, including those to which they have no configured access. Versions 1.13.1 and 1.20.4 contain a patch for this issue. | 6.5 | More Details |
| CVE-2023-29415 | An issue was discovered in libbzip3.a in bzip3 before 1.3.0. A denial of service (process hang) can occur with a crafted archive because bzip3 does not follow the required procedure for interacting with libsais. | 6.5 | More Details |
| CVE-2023-0967 | Bhima version 1.27.0 allows an attacker authenticated with normal user permissions to view sensitive data of other application users and data that should only be viewed by the administrator. This is possible because the application is vulnerable to IDOR, it does not properly validate user permissions with respect to certain actions the user can perform. | 6.5 | More Details |
| CVE-2023-23885 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Contact Form plugin <= 8.0.3.1 versions. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-29416 | An issue was discovered in libbzip3.a in bzip3 before 1.3.0. A bz3_decode_block out-of-bounds write can occur with a crafted archive because bzip3 does not follow the required procedure for interacting with libsais. | 6.5 | More Details |
| CVE-2023-29417 | An issue was discovered in libbzip3.a in bzip3 1.2.2. There is a bz3_decompress out-of-bounds read in certain situations where buffers passed to bzip3 do not contain enough space to be filled with decompressed data. NOTE: the vendor's perspective is that the observed behavior can only occur for a contract violation, and thus the report is invalid. | 6.5 | More Details |
| CVE-2023-29420 | An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is a crash caused by an invalid memmove in bz3_decode_block. | 6.5 | More Details |
| CVE-2023-29419 | An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is a bz3_decode_block out-of-bounds read. | 6.5 | More Details |
| CVE-2023-24411 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Kerry Kline BNE Testimonials plugin <= 2.0.7 versions. | 6.5 | More Details |
| CVE-2023-29418 | An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is an xwrite out-of-bounds read. | 6.5 | More Details |
| CVE-2023-1868 | The YourChannel plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check when clearing the plugin cache via the yrc_clear_cache GET parameter in versions up to, and including, 1.2.3. This makes it possible for unauthenticated attackers to clear the plugin's cache. | 6.5 | More Details |
| CVE-2023-29010 | Budibase is a low code platform for creating internal tools, workflows, and admin panels. Versions prior to 2.4.3 (07 March 2023) are vulnerable to Server-Side Request Forgery. This can lead to an attacker gaining access to a Budibase AWS secret key. Users of Budibase cloud need to take no action. Self-host users who run Budibase on the public internet and are using a cloud provider that allows HTTP access to metadata information should ensure that when they deploy Budibase live, their internal metadata endpoint is not exposed. | 6.5 | More Details |
| CVE-2023-24374 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Photon WP Material Design Icons for Page Builders plugin <= 1.4.2 versions. | 6.5 | More Details |
| CVE-2023-26536 | Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Jonk @ Follow me Darling Sp*tify Play Button for WordPress plugin <= 2.05 versions. | 6.5 | More Details |
| CVE-2023-24378 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Codeat Glossary plugin <= 2.1.27 versions. | 6.5 | More Details |
| CVE-2023-1865 | The YourChannel plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check when resetting plugin settings via the yrc_nuke GET parameter in versions up to, and including, 1.2.3. This makes it possible for unauthenticated attackers to delete YouTube channels from the plugin. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-23815 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Alan Jackson Multi-column Tag Map plugin <= 17.0.24 versions. | 6.5 | More Details |
| CVE-2023-20684 | In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. | 6.4 | More Details |
| CVE-2023-26555 | praecis_parse in ntpd/refclock_palisade.c in NTP 4.2.8p15 has an out-of-bounds write. Any attack method would be complex, e.g., with a manipulated GPS receiver. | 6.4 | More Details |
| CVE-2023-20686 | In display drm, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. | 6.4 | More Details |
| CVE-2023-1552 | ToolboxST prior to version 7.10 is affected by a deserialization vulnerability. An attacker with local access to an HMI or who has conducted a social engineering attack on an authorized operator could execute code in a Toolbox user's context through the deserialization of an untrusted configuration file. Two CVSS scores have been provided to capture the differences between the two aforementioned attack vectors.  Customers are advised to update to ToolboxST 7.10 which can be found in ControlST 7.10. If unable to update at this time customers should ensure they are following the guidance laid out in GE Gas Power's Secure Deployment Guide (GEH-6839). Customers should ensure they are not running ToolboxST as an Administrative user. | 6.4 | More Details |
| CVE-2023-20685 | In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. | 6.4 | More Details |
| CVE-2023-20687 | In display drm, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. | 6.4 | More Details |
| CVE-2023-1949 | A vulnerability, which was classified as critical, was found in PHPGurukul BP Monitoring Management System 1.0. Affected is an unknown function of the file change-password.php of the component Change Password Handler. The manipulation of the argument password leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225336. | 6.3 | More Details |
| CVE-2023-1987 | A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is the function update_order_status of the file /classes/Master.php?f=update_order_status. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225535. | 6.3 | More Details |
| CVE-2023-1986 | A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. Affected is the function delete_order of the file /classes/master.php?f=delete_order. 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-225534 is the identifier assigned to this vulnerability. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1985 | A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. This issue affects the function save_brand of the file /classes/Master.php?f=save_brand. The manipulation of the argument name 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-225533 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1984 | A vulnerability classified as critical was found in SourceCodester Complaint Management System 1.0. This vulnerability affects unknown code of the file /users/check_availability.php of the component POST Parameter Handler. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225532. | 6.3 | More Details |
| CVE-2012-10011 | A vulnerability was found in HD FLV PLayer Plugin up to 1.7 on WordPress. It has been rated as critical. Affected by this issue is the function hd_add_media/hd_update_media of the file functions.php. The manipulation of the argument name leads to sql injection. The attack may be launched remotely. Upgrading to version 1.8 is able to address this issue. The patch is identified as 34d66b9f3231a0e2dc0e536a6fe615d736e863f7. It is recommended to upgrade the affected component. VDB-225350 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1950 | A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file password-recovery.php of the component Password Recovery. The manipulation of the argument emailid/contactno leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225337 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1983 | A vulnerability was found in SourceCodester Sales Tracker Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/products/manage_product.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-225530 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2015-10099 | A vulnerability classified as critical has been found in CP Appointment Calendar Plugin up to 1.1.5 on WordPress. This affects the function dex_process_ready_to_go_appointment of the file dex_appointments.php. The manipulation of the argument itemnumber leads to sql injection. It is possible to initiate the attack remotely. The patch is named e29a9cdbcb0f37d887dd302a05b9e8bf213da01d. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-225351. | 6.3 | More Details |
| CVE-2023-1845 | A vulnerability, which was classified as critical, was found in SourceCodester Online Payroll System 1.0. This affects an unknown part of the file /admin/employee_row.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224985 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1951 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this issue is the function delete_brand of the file /admin/maintenance/brand.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-225338 is the identifier assigned to this vulnerability. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2013-10023 | A vulnerability was found in Editorial Calendar Plugin up to 2.6 on WordPress. It has been declared as critical. Affected by this vulnerability is the function edcal_filter_where of the file edcal.php. The manipulation of the argument edcal_startDate/edcal_endDate leads to sql injection. The attack can be launched remotely. Upgrading to version 2.7 is able to address this issue. The patch is named a9277f13781187daee760b4dfd052b1b68e101cc. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-225151. | 6.3 | More Details |
| CVE-2023-1963 | A vulnerability was found in PHPGurukul Bank Locker Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php of the component Search. The manipulation of the argument searchinput leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225359. | 6.3 | More Details |
| CVE-2023-1855 | A use-after-free flaw was found in xgene_hwmon_remove in drivers/hwmon/xgene-hwmon.c in the Hardware Monitoring Linux Kernel Driver (xgene-hwmon). This flaw could allow a local attacker to crash the system due to a race problem. This vulnerability could even lead to a kernel information leak problem. | 6.3 | More Details |
| CVE-2023-1953 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/sales/index.php. The manipulation of the argument date_start/date_end leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225340. | 6.3 | More Details |
| CVE-2023-1947 | A vulnerability was found in taoCMS 3.0.2. It has been classified as critical. Affected is an unknown function of the file /admin/admin.php. The manipulation leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225330 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1957 | A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=save_sub_category of the component Subcategory Handler. The manipulation of the argument sub_category leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225344. | 6.3 | More Details |
| CVE-2023-1958 | A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file /classes/Master.php?f=delete_sub_category. 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-225345 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1959 | A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This vulnerability affects unknown code of the file /classes/Master.php?f=save_category. The manipulation of the argument category leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-225346 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1960 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Master.php?f=delete_category. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225347. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1954 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been rated as critical. This issue affects the function save_inventory of the file /admin/product/manage.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225341 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1952 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been classified as critical. This affects an unknown part of the file /?p=products of the component Product Search. The manipulation of the argument search leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225339. | 6.3 | More Details |
| CVE-2023-20123 | A vulnerability in the offline access mode of Cisco Duo Two-Factor Authentication for macOS and Duo Authentication for Windows Logon and RDP could allow an unauthenticated, physical attacker to replay valid user session credentials and gain unauthorized access to an affected macOS or Windows device. This vulnerability exists because session credentials do not properly expire. An attacker could exploit this vulnerability by replaying previously used multifactor authentication (MFA) codes to bypass MFA protection. A successful exploit could allow the attacker to gain unauthorized access to the affected device. | 6.3 | More Details |
| CVE-2022-4936 | The WCFM Marketplace plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4.11 due to missing nonce checks on various AJAX actions. This makes it possible for unauthenticated attackers to perform a wide variety of actions such as modifying shipping method details, modifying products, deleting arbitrary posts, and more, via a forged request granted they can trick a site's administrator into performing an action such as clicking on a link. | 6.3 | More Details |
| CVE-2023-1849 | A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/cashadvance_row.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224989 was assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1908 | A vulnerability was found in SourceCodester Simple Mobile Comparison Website 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/categories/view_category.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225150 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1848 | A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/attendance_row.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224988. | 6.3 | More Details |
| CVE-2015-10100 | A vulnerability, which was classified as critical, has been found in Dynamic Widgets Plugin up to 1.5.10 on WordPress. This issue affects some unknown processing of the file classes/dynwid_class.php. The manipulation leads to sql injection. The attack may be initiated remotely. Upgrading to version 1.5.11 is able to address this issue. The identifier of the patch is d0a19c6efcdc86d7093b369bc9e29a0629e57795. It is recommended to upgrade the affected component. The identifier VDB-225353 was assigned to this vulnerability. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1971 | ** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in yuan1994 tpAdmin 1.3.12. Affected is the function remote of the file application\admin\controller\Upload.php. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225408. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. | 6.3 | More Details |
| CVE-2023-1885 | Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 6.3 | More Details |
| CVE-2023-1847 | A vulnerability was found in SourceCodester Online Payroll System 1.0 and classified as critical. This issue affects some unknown processing of the file attendance.php. The manipulation of the argument employee leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224987. | 6.3 | More Details |
| CVE-2022-4937 | The WCFM Frontend Manager plugin for WordPress is vulnerable to unauthorized modification and access of data in versions up to, and including, 6.6.0 due to missing capability checks on various AJAX actions. This makes it possible for authenticated attackers, with minimal permissions such as subscribers, to perform a wide variety of actions such as modifying knowledge bases, modifying notices, modifying payments, managing vendors, capabilities, and so much more. There were hundreds of AJAX endpoints affected. | 6.3 | More Details |
| CVE-2023-1856 | A vulnerability has been found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/transactions/track_shipment.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224995. | 6.3 | More Details |
| CVE-2022-4938 | The WCFM Frontend Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.6.0 due to missing nonce checks on various AJAX actions. This makes it possible for unauthenticated attackers to perform a wide variety of actions such as modifying knowledge bases, modifying notices, modifying payments, managing vendors, capabilities, and so much more, via a forged request granted they can trick a site's administrator into performing an action such as clicking on a link. There were hundreds of AJAX endpoints affected. | 6.3 | More Details |
| CVE-2023-1970 | ** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as problematic, has been found in yuan1994 tpAdmin 1.3.12. This issue affects the function Upload of the file application\admin\controller\Upload.php. The manipulation of the argument file leads to unrestricted upload. 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-225407. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. | 6.3 | More Details |
| CVE-2023-1846 | A vulnerability has been found in SourceCodester Online Payroll System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/deduction_row.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-224986 is the identifier assigned to this vulnerability. | 6.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-4941 | The WCFM Membership plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.9.10 due to missing nonce checks on various AJAX actions. This makes it possible for unauthenticated attackers to perform a wide variety of actions such as modifying membership details, changing renewal information, controlling membership approvals, and more, via a forged request granted they can trick a site's administrator into performing an action such as clicking on a link. | 6.3 | More Details |
| CVE-2023-1969 | A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects unknown code of the file /admin/inventory/manage_stock.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-225406 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-1940 | A vulnerability classified as critical was found in SourceCodester Simple and Beautiful Shopping Cart System 1.0. This vulnerability affects unknown code of the file delete_user_query.php. The manipulation of the argument user_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225316. | 6.3 | More Details |
| CVE-2023-1942 | A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/?page=user of the component Avatar Handler. The manipulation leads to unrestricted upload. 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-225319. | 6.3 | More Details |
| CVE-2023-1850 | A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-224990 is the identifier assigned to this vulnerability. | 6.3 | More Details |
| CVE-2023-23588 | A vulnerability has been identified in SIMATIC IPC1047 (All versions), SIMATIC IPC1047E (All versions with maxView Storage Manager < 4.09.00.25611 on Windows), SIMATIC IPC647D (All versions), SIMATIC IPC647E (All versions with maxView Storage Manager < 4.09.00.25611 on Windows), SIMATIC IPC847D (All versions), SIMATIC IPC847E (All versions with maxView Storage Manager < 4.09.00.25611 on Windows). The Adaptec Maxview application on affected devices is using a non-unique TLS certificate across installations to protect the communication from the local browser to the local application. A local attacker may use this key to decrypt intercepted local traffic between the browser and the application and could perform a man-in-the-middle attack in order to modify data in transit. | 6.2 | More Details |
| CVE-2023-28269 | Windows Boot Manager Security Feature Bypass Vulnerability | 6.2 | More Details |
| CVE-2023-28249 | Windows Boot Manager Security Feature Bypass Vulnerability | 6.2 | More Details |
| CVE-2023-28341 | Stored Cross site scripting (XSS) vulnerability in Zoho ManageEngine Applications Manager through 16340 allows an unauthenticated user to inject malicious javascript on the incorrect login details page. | 6.1 | More Details |
| CVE-2023-23277 | Snippet-box 1.0.0 is vulnerable to Cross Site Scripting (XSS). Remote attackers can render arbitrary web script or HTML from the "Snippet code" form field. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-31889 | Cross Site Scripting (XSS) vulnerability in audit/templates/auditlogs.tmpl.php in osTicket osTicket-plugins before commit a7842d494889fd5533d13deb3c6a7789768795ae. | 6.1 | More Details |
| CVE-2023-27499 | SAP GUI for HTML - versions KERNEL 7.22, 7.53, 7.54, 7.77, 7.81, 7.85, 7.89, 7.91, KRNL64UC, 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT does not sufficiently encode user-controlled inputs, resulting in a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could craft a malicious URL and lure the victim to click, the script supplied by the attacker will execute in the victim user's browser. The information from the victim's web browser can either be modified or read and sent to the attacker. | 6.1 | More Details |
| CVE-2023-0983 | The stylish-cost-calculator-premium WordPress plugin before 7.9.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Stored Cross-Site Scripting which could be used against admins when viewing submissions submitted through the Email Quote Form. | 6.1 | More Details |
| CVE-2023-26788 | Veritas Appliance v4.1.0.1 is affected by Host Header Injection attacks. HTTP host header can be manipulated and cause the application to behave in unexpected ways. Any changes made to the header would just cause the request to be sent to a completely different Domain/IP address. | 6.1 | More Details |
| CVE-2022-39048 | A XSS vulnerability was identified in the ServiceNow UI page assessment_redirect. To exploit this vulnerability, an attacker would need to persuade an authenticated user to click a maliciously crafted URL. Successful exploitation potentially could be used to conduct various client-side attacks, including, but not limited to, phishing, redirection, theft of CSRF tokens, and use of an authenticated user's browser or session to attack other systems. | 6.1 | More Details |
| CVE-2023-26773 | Cross Site Scripting vulnerability found in Sales Tracker Management System v.1.0 allows a remote attacker to gain privileges via the product list function in the Master.php file. | 6.1 | More Details |
| CVE-2023-22985 | Sourcecodester Simple Guestbook Management System version 1 is vulnerable to Cross Site Scripting (XSS) via Name, Referrer, Location, and Comments. | 6.1 | More Details |
| CVE-2023-20147 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2022-3513 | An issue has been discovered in GitLab affecting all versions starting from 12.8 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. A specially crafted payload could lead to a reflected XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims on self-hosted instances running without strict CSP. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-29016 | The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. A cross-site scripting vulnerability has been identified in Goobi viewer core prior to version 23.03 when using nicknames. An attacker could create a user account and enter malicious scripts into their profile's nickname, resulting in the execution in the user's browser when displaying the nickname on certain pages. The vulnerability has been fixed in version 23.03. | 6.1 | More Details |
| CVE-2023-28314 | Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability | 6.1 | More Details |
| CVE-2023-28313 | Microsoft Dynamics 365 Customer Voice Cross-Site Scripting Vulnerability | 6.1 | More Details |
| CVE-2023-28069 | Dell Streaming Data Platform prior to 1.4 contains Open Redirect vulnerability. A remote unauthenticated attacker can phish the legitimate user to redirect to malicious website leading to information disclosure and launch of phishing attacks. | 6.1 | More Details |
| CVE-2023-26789 | Veritas NetBackUp OpsCenter Version 9.1.0.1 is vulnerable to Reflected Cross-site scripting (XSS). The Web App fails to adequately sanitize special characters. By leveraging this issue, an attacker is able to cause arbitrary HTML and JavaScript code to be executed in a user's browser. | 6.1 | More Details |
| CVE-2023-20068 | A vulnerability in the web-based management interface of Cisco Prime Infrastructure Software could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of the web-based management interface on an affected device to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information. | 6.1 | More Details |
| CVE-2023-1880 | Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 6.1 | More Details |
| CVE-2023-1884 | Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 6.1 | More Details |
| CVE-2023-28639 | GLPI is a free asset and IT management software package. Starting in version 0.85 and prior to versions 9.5.13 and 10.0.7, a malicious link can be crafted by an unauthenticated user. It will be able to exploit a reflected XSS in case any authenticated user opens the crafted link. This issue is fixed in versions 9.5.13 and 10.0.7. | 6.1 | More Details |
| CVE-2023-24935 | Microsoft Edge (Chromium-based) Spoofing Vulnerability | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20137 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20138 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20139 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20140 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20141 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-1916 | A flaw was found in tiffcrop, a program distributed by the libtiff package. A specially crafted tiff file can lead to an out-of-bounds read in the extractImageSection function in tools/tiffcrop.c, resulting in a denial of service and limited information disclosure. This issue affects libtiff versions 4.x. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20148 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20143 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20142 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-29014 | The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. A reflected cross-site scripting vulnerability has been identified in Goobi viewer core prior to version 23.03 when evaluating the LOGID parameter. An attacker could trick a user into following a specially crafted link to a Goobi viewer installation, resulting in the execution of malicious script code in the user's browser. The vulnerability has been fixed in version 23.03. | 6.1 | More Details |
| CVE-2023-20145 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20144 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20146 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20149 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20150 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-20151 | Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. | 6.1 | More Details |
| CVE-2023-29015 | The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. A cross-site scripting vulnerability has been identified in the user comment feature of Goobi viewer core prior to version 23.03. An attacker could create a specially crafted comment, resulting in the execution of malicious script code in the user's browser when displaying the comment. The vulnerability has been fixed in version 23.03. | 6.1 | More Details |
| CVE-2023-20021 | Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. | 6.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20022 | Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. | 6.0 | More Details |
| CVE-2023-20023 | Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. | 6.0 | More Details |
| CVE-2023-27897 | In SAP CRM - versions 700, 701, 702, 712, 713, an attacker who is authenticated with a non-administrative role and a common remote execution authorization can use a vulnerable interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or application data and application availability. | 6.0 | More Details |
| CVE-2023-20030 | A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access sensitive information, conduct a server-side request forgery (SSRF) attack through an affected device, or negatively impact the responsiveness of the web-based management interface itself. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of confidential information. A successful exploit could also cause the web application to perform arbitrary HTTP requests on behalf of the attacker or consume memory resources to reduce the availability of the web-based management interface. To successfully exploit this vulnerability, an attacker would need valid Super Admin or Policy Admin credentials. | 6.0 | More Details |
| CVE-2023-20152 | Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. | 6.0 | More Details |
| CVE-2023-20122 | Multiple vulnerabilities in the restricted shell of Cisco Evolved Programmable Network Manager (EPNM), Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to escape the restricted shell and gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. | 6.0 | More Details |
| CVE-2023-20121 | Multiple vulnerabilities in the restricted shell of Cisco Evolved Programmable Network Manager (EPNM), Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to escape the restricted shell and gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. | 6.0 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20153 | Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. | 6.0 | More Details |
| CVE-2023-24002 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart YouTube Embed, Playlist and Popup by WpDevArt plugin <= 2.6.3 versions. | 5.9 | More Details |
| CVE-2022-43293 | Wacom Driver 6.3.46-1 for Windows was discovered to contain an arbitrary file write vulnerability via the component \Wacom\Wacom_Tablet.exe. | 5.9 | More Details |
| CVE-2023-23971 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CodePeople WP Time Slots Booking Form plugin <= 1.1.81 versions. | 5.9 | More Details |
| CVE-2023-24396 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in E4J s.R.L. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.11 versions. | 5.9 | More Details |
| CVE-2023-23972 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Smplug-in Social Like Box and Page by WpDevArt plugin <= 0.8.39 versions. | 5.9 | More Details |
| CVE-2023-23987 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPEverest User Registration plugin <= 2.3.0 versions. | 5.9 | More Details |
| CVE-2023-23996 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.3 versions. | 5.9 | More Details |
| CVE-2023-23998 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in E4J s.R.L. VikRentCar Car Rental Management System plugin <= 1.3.0 versions. | 5.9 | More Details |
| CVE-2023-24001 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Yannick Lefebvre Modal Dialog plugin <= 3.5.9 versions. | 5.9 | More Details |
| CVE-2023-1802 | In Docker Desktop 4.17.x the Artifactory Integration falls back to sending registry credentials over plain HTTP if the HTTPS health check has failed. A targeted network sniffing attack can lead to a disclosure of sensitive information. Only users who have Access Experimental Features enabled and have logged in to a private registry are affected. | 5.9 | More Details |
| CVE-2023-24006 | Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Link Software LLC WP Terms Popup plugin <= 2.6.0 versions. | 5.9 | More Details |
| CVE-2023-25062 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PINPOINT.WORLD Pinpoint Booking System plugin <= 2.9.9.2.8 versions. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-24403 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP For The Win bbPress Voting plugin <= 2.1.11.0 versions. | 5.9 | More Details |
| CVE-2023-24387 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions. | 5.9 | More Details |
| CVE-2023-24383 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Namaste! LMS plugin <= 2.5.9.1 versions. | 5.9 | More Details |
| CVE-2023-23981 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in QuantumCloud Conversational Forms for ChatBot plugin <= 1.1.6 versions. | 5.9 | More Details |
| CVE-2023-23982 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPGear.Pro WPFrom Email plugin <= 1.8.8 versions. | 5.9 | More Details |
| CVE-2023-24004 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Image and Video Lightbox, Image PopUp plugin <= 2.1.5 versions. | 5.9 | More Details |
| CVE-2023-28828 | A vulnerability has been identified in Polarion ALM (All versions < V22R2). The application contains a XML External Entity Injection (XXE) vulnerability. This could allow an attacker to view files on the application server filesystem. | 5.9 | More Details |
| CVE-2023-23994 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marcel Bootsman Auto Hide Admin Bar plugin <= 1.6.1 versions. | 5.9 | More Details |
| CVE-2023-23980 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in MailOptin Popup Builder Team MailOptin plugin <= 1.2.54.0 versions. | 5.9 | More Details |
| CVE-2023-25464 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in StreamWeasels Twitch Player plugin <= 2.1.0 versions. | 5.9 | More Details |
| CVE-2023-25059 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in avalex GmbH avalex – Automatically secure legal texts plugin <= 3.0.3 versions. | 5.9 | More Details |
| CVE-2023-24402 | Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Veribo, Roland Murg WP Booking System – Booking Calendar plugin <= 2.0.18 versions. | 5.9 | More Details |
| CVE-2023-25046 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Podlove Podlove Podcast Publisher plugin <= 3.8.2 versions. | 5.9 | More Details |
| CVE-2023-25392 | Allegro Tech BigFlow <1.6 is vulnerable to Missing SSL Certificate Validation. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25442 | Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in Marcel Pol Zeno Font Resizer plugin <= 1.7.9 versions. | 5.9 | More Details |
| CVE-2023-23799 | Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in Leonardo Giacone Easy Panorama plugin <= 1.1.4 versions. | 5.9 | More Details |
| CVE-2023-29094 | Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in PI Websolution Product page shipping calculator for WooCommerce plugin <= 1.3.20 versions. | 5.9 | More Details |
| CVE-2023-24398 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Snap Creek Software EZP Coming Soon Page plugin <= 1.0.7.3 versions. | 5.9 | More Details |
| CVE-2023-25712 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP-Buddy Google Analytics Opt-Out plugin <= 2.3.4 versions. | 5.9 | More Details |
| CVE-2023-29170 | Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in PI Websolution Product Enquiry for WooCommerce, WooCommerce product catalog plugin <= 2.2.12 versions. | 5.9 | More Details |
| CVE-2023-25705 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Go Prayer WP Prayer plugin <= 1.9.6 versions. | 5.9 | More Details |
| CVE-2023-25702 | Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in Fullworks Quick Paypal Payments plugin <= 5.7.25 versions. | 5.9 | More Details |
| CVE-2023-25022 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Watu Quiz plugin <= 3.3.8 versions. | 5.9 | More Details |
| CVE-2023-25027 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Chained Quiz plugin <= 1.3.2.5 versions. | 5.9 | More Details |
| CVE-2022-34333 | IBM Sterling Order Management 10.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 229698. | 5.9 | More Details |
| CVE-2023-25716 | Auth (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gqevu6bsiz Announce from the Dashboard plugin <= 1.5.1 versions. | 5.9 | More Details |
| CVE-2023-25049 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in impleCode eCommerce Product Catalog Plugin for WordPress plugin <= 3.3.4 versions. | 5.9 | More Details |
| CVE-2023-25023 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Saleswonder.Biz Webinar ignition plugin <= 2.14.2 versions. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25024 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Icegram Icegram Collect plugin <= 1.3.8 versions. | 5.9 | More Details |
| CVE-2023-25031 | Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.1 versions. | 5.9 | More Details |
| CVE-2023-1098 | An information disclosure vulnerability has been discovered in GitLab EE/CE affecting all versions starting from 11.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 will allow an admin to leak password from repository mirror configuration. | 5.8 | More Details |
| CVE-2023-1733 | A denial of service condition exists in the Prometheus server bundled with GitLab affecting all versions from 11.10 to 15.8.5, 15.9 to 15.9.4 and 15.10 to 15.10.1. | 5.8 | More Details |
| CVE-2023-0319 | An issue has been discovered in GitLab affecting all versions starting from 13.6 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1, allowing to read environment names supposed to be restricted to project memebers only. | 5.8 | More Details |
| CVE-2023-25711 | Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPGlobus WPGlobus Translate Options plugin <= 2.1.0 versions. | 5.8 | More Details |
| CVE-2023-20051 | A vulnerability in the Vector Packet Processor (VPP) of Cisco Packet Data Network Gateway (PGW) could allow an unauthenticated, remote attacker to stop ICMP traffic from being processed over an IPsec connection. This vulnerability is due to the VPP improperly handling a malformed packet. An attacker could exploit this vulnerability by sending a malformed Encapsulating Security Payload (ESP) packet over an IPsec connection. A successful exploit could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS). | 5.8 | More Details |
| CVE-2023-28368 | TP-Link L2 switch T2600G-28SQ firmware versions prior to 'T2600G-28SQ(UN)_V1_1.0.6 Build 20230227' uses vulnerable SSH host keys. A fake device may be prepared to spoof the affected device with the vulnerable host key.If the administrator may be tricked to login to the fake device, the credential information for the affected device may be obtained. | 5.7 | More Details |
| CVE-2023-1708 | An issue was identified in GitLab CE/EE affecting all versions from 1.0 prior to 15.8.5, 15.9 prior to 15.9.4, and 15.10 prior to 15.10.1 where non-printable characters gets copied from clipboard, allowing unexpected commands to be executed on victim machine. | 5.7 | More Details |
| CVE-2023-26551 | mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write in the cp<cpdec while loop. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. | 5.6 | More Details |
| CVE-2023-26554 | mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write when adding a '\0' character. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. | 5.6 | More Details |
| CVE-2023-26553 | mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write when copying the trailing number. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. | 5.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-26552 | mstolfp in libntp/mstolfp.c in NTP 4.2.8p15 has an out-of-bounds write when adding a decimal point. An adversary may be able to attack a client ntpq process, but cannot attack ntpd. | 5.6 | More Details |
| CVE-2022-47335 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2023-29465 | SageMath FlintQS 1.0 relies on pathnames under TMPDIR (typically world-writable), which (for example) allows a local user to overwrite files with the privileges of a different user (who is running FlintQS). | 5.5 | More Details |
| CVE-2022-47336 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2022-47337 | In media service, there is a missing permission check. This could lead to local denial of service in media service. | 5.5 | More Details |
| CVE-2022-47463 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2022-47464 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2022-47465 | In vdsp service, there is a missing permission check. This could lead to local denial of service in vdsp service. | 5.5 | More Details |
| CVE-2022-47466 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2022-47467 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2022-47468 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |
| CVE-2020-24736 | Buffer Overflow vulnerability found in SQLite3 v.3.27.1 and before allows a local attacker to cause a denial of service via a crafted script. | 5.5 | More Details |
| CVE-2022-43309 | Supermicro X11SSL-CF HW Rev 1.01, BMC firmware v1.63 was discovered to contain insecure permissions. | 5.5 | More Details |
| CVE-2022-47362 | In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service. | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0838 | An issue has been discovered in GitLab affecting versions starting from 15.1 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. A maintainer could modify a webhook URL to leak masked webhook secrets by adding a new parameter to the url. This addresses an incomplete fix for CVE-2022-4342. | 5.5 | More Details |
| CVE-2023-28228 | Windows Spoofing Vulnerability | 5.5 | More Details |
| CVE-2023-23898 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in CreativeThemes Blocksy Companion plugin <= 1.8.67 versions. | 5.5 | More Details |
| CVE-2023-29576 | Bento4 v1.6.0-639 was discovered to contain a segmentation violation via the AP4_TrunAtom::SetDataOffset(int) function in Ap4TrunAtom.h. | 5.5 | More Details |
| CVE-2023-28299 | Visual Studio Spoofing Vulnerability | 5.5 | More Details |
| CVE-2023-28298 | Windows Kernel Denial of Service Vulnerability | 5.5 | More Details |
| CVE-2023-23891 | Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme installed and activated. | 5.5 | More Details |
| CVE-2023-1869 | The YourChannel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 1.2.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrative-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. | 5.5 | More Details |
| CVE-2023-28271 | Windows Kernel Memory Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2023-28266 | Windows Common Log File System Driver Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2023-28263 | Visual Studio Information Disclosure Vulnerability | 5.5 | More Details |
| CVE-2022-46703 | A logic issue was addressed with improved restrictions. This issue is fixed in iOS 15.7.2 and iPadOS 15.7.2, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2. An app may be able to read sensitive location information | 5.5 | More Details |
| CVE-2023-28253 | Windows Kernel Information Disclosure Vulnerability | 5.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-25955 | National land numerical information data conversion tool all versions improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the PC may be accessed by an attacker. | 5.5 | More Details |
| CVE-2023-1758 | Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 5.4 | More Details |
| CVE-2023-1881 | Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.3. | 5.4 | More Details |
| CVE-2023-24747 | Jfinal CMS v5.1 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /system/dict/list. | 5.4 | More Details |
| CVE-2023-20134 | Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack or upload arbitrary files as recordings. For more information about these vulnerabilities, see the Details section of this advisory. | 5.4 | More Details |
| CVE-2023-1726 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proliz OBS allows Stored XSS for an authenticated user.This issue affects OBS: before 23.04.01. | 5.4 | More Details |
| CVE-2023-1883 | Improper Access Control in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 5.4 | More Details |
| CVE-2023-0523 | An issue has been discovered in GitLab affecting all versions starting from 15.6 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. An XSS was possible via a malicious email address for certain instances. | 5.4 | More Details |
| CVE-2023-1882 | Cross-site Scripting (XSS) - DOM in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 5.4 | More Details |
| CVE-2023-1956 | A vulnerability classified as critical was found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=delete_img of the component Image Handler. The manipulation of the argument path leads to path traversal. 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-225343. | 5.4 | More Details |
| CVE-2023-20096 | A vulnerability in the web-based management interface of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack. This vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by entering crafted text into various input fields within the web-based management interface. A successful exploit could allow the attacker to perform a stored XSS attack, which could allow the execution of scripts within the context of other users of the interface. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1866 | The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the clearKeys function. This makes it possible for unauthenticated attackers to reset the plugin's channel settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 5.4 | More Details |
| CVE-2023-1757 | Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 5.4 | More Details |
| CVE-2023-1867 | The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the save function. This makes it possible for unauthenticated attackers to change the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 5.4 | More Details |
| CVE-2023-26260 | OXID eShop 6.2.x before 6.4.4 and 6.5.x before 6.5.2 allows session hijacking, leading to partial access of a customer's account by an attacker, due to an improper check of the user agent. | 5.4 | More Details |
| CVE-2023-1878 | Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 5.4 | More Details |
| CVE-2023-20132 | Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack or upload arbitrary files as recordings. For more information about these vulnerabilities, see the Details section of this advisory. | 5.4 | More Details |
| CVE-2023-1871 | The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the deleteLang function. This makes it possible for unauthenticated attackers to reset the plugin's quick language translation settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 5.4 | More Details |
| CVE-2022-33959 | IBM Sterling Order Management 10.0 could allow a user to bypass validation and perform unauthorized actions on behalf of other users. IBM X-Force ID: 229320. | 5.4 | More Details |
| CVE-2023-1879 | Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 5.4 | More Details |
| CVE-2023-26467 | A man in the middle can redirect traffic to a malicious server in a compromised configuration. | 5.4 | More Details |
| CVE-2023-0363 | The Scheduled Announcements Widget WordPress plugin before 1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. | 5.4 | More Details |
| CVE-2022-46793 | Cross-Site Request Forgery (CSRF) vulnerability in AdTribes.Io Product Feed PRO for WooCommerce plugin <= 12.4.4 versions. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-26847 | A stored cross-site scripting (XSS) vulnerability in OpenCATS v0.9.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the state parameter at opencats/index.php?m=candidates. | 5.4 | More Details |
| CVE-2023-24464 | Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier | 5.4 | More Details |
| CVE-2023-0546 | The Contact Form Plugin WordPress plugin before 4.3.25 does not properly sanitize and escape the srcdoc attribute in iframes in it's custom HTML field type, allowing a logged in user with roles as low as contributor to inject arbitrary javascript into a form which will trigger for any visitor to the form or admins previewing or editing the form. | 5.4 | More Details |
| CVE-2023-29376 | An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potential XSS by privileged users in Sitefinity to media libraries. | 5.4 | More Details |
| CVE-2022-4827 | The WP Tiles WordPress plugin through 1.1.2 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-2023-24181 | LuCI openwrt-22.03 branch git-22.361.69894-438c598 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /openvpn/pageswitch.htm. | 5.4 | More Details |
| CVE-2022-37462 | A stored Cross-Site Scripting (XSS) vulnerability in the Chat gadget in Upstream Works Agent Desktop for Cisco Finesse through 4.2.12 and 5.0 allows remote attackers to inject arbitrary web script or HTML via AttachmentId in the file-upload details. | 5.4 | More Details |
| CVE-2023-26846 | A stored cross-site scripting (XSS) vulnerability in OpenCATS v0.9.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the city parameter at opencats/index.php?m=candidates. | 5.4 | More Details |
| CVE-2023-0580 | Insecure Storage of Sensitive Information vulnerability in ABB My Control System (on-premise) allows an attacker who successfully exploited this vulnerability to gain access to the secure application data or take control of the application. Of the services that make up the My Control System (on-premise) application, the following ones are affected by this vulnerability: User Interface System Monitoring1 Asset Inventory This issue affects My Control System (on-premise): from 5.0;0 through 5.13. | 5.4 | More Details |
| CVE-2023-29189 | SAP CRM (WebClient UI) - versions S4FND 102, 103, 104, 105, 106, 107, WEBCUIF, 700, 701, 731, 730, 746, 747, 748, 800, 801, allows an authenticated attacker to modify HTTP verbs used in requests to the web server. This application is exposed over the network and successful exploitation can lead to exposure of form fields | 5.4 | More Details |
| CVE-2022-43770 | Hitachi Vantara Pentaho Business Analytics Server versions before 9.3.0.0, 9.2.0.4 and 8.3.0.27 does not correctly perform an authorization check in the dashboard editor plugin API. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-24182 | LuCI openwrt-22.03 branch git-22.361.69894-438c598 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the component /system/sshkeys.js. | 5.4 | More Details |
| CVE-2023-26120 | This affects all versions of the package com.xuxueli:xxl-job. HTML uploaded payload executed successfully through /xxl-job-admin/user/add and /xxl-job-admin/user/update. | 5.4 | More Details |
| CVE-2023-24721 | A cross-site scripting (XSS) vulnerability in LiveAction LiveSP v21.1.2 allows attackers to execute arbitrary web scripts or HTML. | 5.4 | More Details |
| CVE-2023-0842 | xml2js version 0.4.23 allows an external attacker to edit or add new properties to an object. This is possible because the application does not properly validate incoming JSON keys, thus allowing the __proto__ property to be edited. | 5.3 | More Details |
| CVE-2023-29185 | SAP NetWeaver AS for ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters in certain circumstances which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. | 5.3 | More Details |
| CVE-2023-25415 | Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. The device allows unauthenticated access to Event Notification configuration. | 5.3 | More Details |
| CVE-2023-25414 | Aten PE8108 2.4.232 is vulnerable to denial of service (DOS). | 5.3 | More Details |
| CVE-2023-28226 | Windows Enroll Engine Security Feature Bypass Vulnerability | 5.3 | More Details |
| CVE-2023-0645 | An out of bounds read exists in libjxl. An attacker using a specifically crafted file could cause an out of bounds read in the exif handler. We recommend upgrading to version 0.8.1 or past commit https://github.com/libjxl/libjxl/pull/2101/commits/d95b050c1822a5b1ede9e0dc937e43fca1b10159 https://github.com/libjxl/libjxl/pull/2101/commits/d95b050c1822a5b1ede9e0dc937e43fca1b10159 | 5.3 | More Details |
| CVE-2023-20073 | A vulnerability in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to upload arbitrary files to an affected device. This vulnerability is due to insufficient authorization enforcement mechanisms in the context of file uploads. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to upload arbitrary files to the affected device. | 5.3 | More Details |
| CVE-2023-30465 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.5.0. By manipulating the "orderType" parameter and the ordering of the returned content using an SQL injection attack, an attacker can extract the username of the user with ID 1 from the "user" table, one character at a time. Users are advised to upgrade to Apache InLong's 1.6.0 or cherry-pick [1] to solve it. https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html [1] https://github.com/apache/inlong/issues/7529 https://github.com/apache/inlong/issues/7529 | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27464 | A vulnerability has been identified in Mendix Forgot Password (Mendix 7 compatible) (All versions < V3.7.1), Mendix Forgot Password (Mendix 8 compatible) (All versions < V4.1.1), Mendix Forgot Password (Mendix 9 compatible) (All versions < V5.1.1). The affected versions of the module contain an observable response discrepancy issue that could allow an attacker to retrieve sensitive information. | 5.3 | More Details |
| CVE-2023-24527 | SAP NetWeaver AS Java for Deploy Service - version 7.5, does not perform any access control checks for functionalities that require user identity enabling an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access a service which will enable them to access but not modify server settings and data with no effect on availability and integrity. | 5.3 | More Details |
| CVE-2022-43951 | An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] 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 may allow an unauthenticated attacker to access sensitive information via crafted HTTP requests. | 5.3 | More Details |
| CVE-2023-1710 | A sensitive information disclosure vulnerability in GitLab affecting all versions from 15.0 prior to 15.8.5, 15.9 prior to 15.9.4 and 15.10 prior to 15.10.1 allows an attacker to view the count of internal notes for a given issue. | 5.3 | More Details |
| CVE-2023-1167 | Improper authorization in Gitlab EE affecting all versions from 12.3.0 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 allows an unauthorized access to security reports in MR. | 5.3 | More Details |
| CVE-2023-29108 | The IP filter in ABAP Platform and SAP Web Dispatcher - versions WEBDISP 7.85, 7.89, KERNEL 7.85, 7.89, 7.91, may be vulnerable by erroneous IP netmask handling. This may enable access to backend applications from unwanted sources. | 5.0 | More Details |
| CVE-2022-43947 | An improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiOS version 7.2.0 through 7.2.3 and before 7.0.10, FortiProxy version 7.2.0 through 7.2.2 and before 7.0.8 administrative interface allows an attacker with a valid user account to perform brute-force attacks on other user accounts via injecting valid login sessions. | 5.0 | More Details |
| CVE-2023-20103 | A vulnerability in Cisco Secure Network Analytics could allow an authenticated, remote attacker to execute arbitrary code as a root user on an affected device. This vulnerability is due to insufficient validation of user input to the web interface. An attacker could exploit this vulnerability by uploading a crafted file to an affected device. A successful exploit could allow the attacker to execute code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. | 4.9 | More Details |
| CVE-2022-43928 | The IBM Toolbox for Java (Db2 Mirror for i 7.4 and 7.5) could allow a user to obtain sensitive information, caused by utilizing a Java string for processing. Since Java strings are immutable, their contents exist in memory until garbage collected. This means sensitive data could be visible in memory over an indefinite amount of time. IBM has addressed this issue by reducing the amount of time the sensitive data is visible in memory. IBM X-Force ID: 241675. | 4.9 | More Details |
| CVE-2023-27802 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EditvsList parameter at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-27801 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DelDNSHnList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-27806 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the ipqos_lanip_dellist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-0156 | The All-In-One Security (AIOS) WordPress plugin before 5.1.5 does not limit what log files to display in it's settings pages, allowing an authorized user (admin+) to view the contents of arbitrary files and list directories anywhere on the server (to which the web server has access). The plugin only displays the last 50 lines of the file. | 4.9 | More Details |
| CVE-2023-27803 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EdittriggerList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-27804 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DelvsList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-28277 | Windows DNS Server Information Disclosure Vulnerability | 4.9 | More Details |
| CVE-2023-27805 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EditSTList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-27810 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the ipqos_lanip_editlist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-27808 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DeltriggerList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-27807 | H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the Delstlist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. | 4.9 | More Details |
| CVE-2023-28852 | GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to versions 9.5.13 and 10.0.7, a user with dashboard administration rights may hack the dashboard form to store malicious code that will be executed when other users will use the related dashboard. Versions 9.5.13 and 10.0.7 contain a patch for this issue. | 4.8 | More Details |
| CVE-2023-0605 | The Auto Rename Media On Upload WordPress plugin before 1.1.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). | 4.8 | More Details |
| CVE-2023-0893 | The Time Sheets WordPress plugin before 1.29.3 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-2023-0157 | The All-In-One Security (AIOS) WordPress plugin before 5.1.5 does not escape the content of log files before outputting it to the plugin admin page, allowing an authorized user (admin+) to plant bogus log files containing malicious JavaScript code that will be executed in the context of any administrator visiting this page. | 4.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-0423 | The WordPress Amazon S3 Plugin WordPress plugin before 1.6 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 | 4.8 | More Details |
| CVE-2023-0874 | The Klaviyo WordPress plugin before 3.0.10 does not sanitize 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-2023-0422 | The Article Directory WordPress plugin through 1.3 does not properly sanitize the `publish_terms_text` setting before displaying it in the administration panel, which may enable administrators to conduct Stored XSS attacks in multisite contexts. | 4.8 | More Details |
| CVE-2023-1120 | The Simple Giveaways WordPress plugin before 2.45.1 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-2023-1121 | The Simple Giveaways WordPress plugin before 2.45.1 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-2023-1122 | The Simple Giveaways WordPress plugin before 2.45.1 does not sanitise and escape some of its Giveaways options, 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-2023-23572 | Cross-site scripting vulnerability in SEIKO EPSON printers/network interface Web Config allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers/network interface via a web browser. According to SEIKO EPSON CORPORATION, it is also called as Remote Manager in some products. Web Config is pre-installed in some printers/network interface provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor. | 4.8 | More Details |
| CVE-2023-1854 | A vulnerability, which was classified as problematic, was found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file admin/. The manipulation leads to session expiration. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-224994 is the identifier assigned to this vulnerability. | 4.7 | More Details |
| CVE-2023-1582 | A race problem was found in fs/proc/task_mmu.c in the memory management sub-component in the Linux kernel. This issue may allow a local attacker with user privilege to cause a denial of service. | 4.7 | More Details |
| CVE-2023-1756 | Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 4.7 | More Details |
| CVE-2023-1909 | A vulnerability, which was classified as critical, was found in PHPGurukul BP Monitoring Management System 1.0. Affected is an unknown function of the file profile.php of the component User Profile Update Handler. The manipulation of the argument name/mobno 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-225318 is the identifier assigned to this vulnerability. | 4.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-43914 | IBM TRIRIGA Application Platform 4.0 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: 241036. | 4.6 | More Details |
| CVE-2023-28636 | GLPI is a free asset and IT management software package. Starting in version 0.60 and prior to versions 9.5.13 and 10.0.7, a vulnerability allows an administrator to create a malicious external link. This issue is fixed in versions 9.5.13 and 10.0.7. | 4.5 | More Details |
| CVE-2023-28276 | Windows Group Policy Security Feature Bypass Vulnerability | 4.4 | More Details |
| CVE-2023-1913 | The Maps Widget for Google Maps for WordPress is vulnerable to Stored Cross-Site Scripting via widget settings in versions up to, and including, 4.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. | 4.4 | More Details |
| CVE-2023-20660 | In wlan, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. | 4.4 | More Details |
| CVE-2023-20665 | In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. | 4.4 | More Details |
| CVE-2023-29109 | The SAP Application Interface Framework (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows an Excel formula injection. An authorized attacker can inject arbitrary Excel formulas into fields like the Tooltip of the Custom Hints List. Once the victim opens the downloaded Excel document, the formula will be executed. As a result, an attacker can cause limited impact on the confidentiality and integrity of the application. | 4.4 | More Details |
| CVE-2023-20688 | In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. | 4.4 | More Details |
| CVE-2023-20674 | In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. | 4.4 | More Details |
| CVE-2023-20675 | In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588569. | 4.4 | More Details |
| CVE-2020-11935 | It was discovered that aufs improperly managed inode reference counts in the vfsub_dentry_open() method. A local attacker could use this vulnerability to cause a denial of service attack. | 4.4 | More Details |
| CVE-2023-20676 | In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07628518. | 4.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-20679 | In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. | 4.4 | More Details |
| CVE-2023-20677 | In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. | 4.4 | More Details |
| CVE-2023-28284 | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability | 4.3 | More Details |
| CVE-2023-1870 | The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the saveLang function. This makes it possible for unauthenticated attackers to change the plugin's quick language translation settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1858 | A vulnerability was found in SourceCodester Earnings and Expense Tracker App 1.0. It has been classified as problematic. This affects an unknown part of the file index.php. The manipulation of the argument page leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-224997 was assigned to this vulnerability. | 4.3 | More Details |
| CVE-2023-23801 | Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Really Simple Google Tag Manager plugin <= 1.0.6 versions. | 4.3 | More Details |
| CVE-2023-23575 | Improper access control vulnerability in CONPROSYS IoT Gateway products allows a remote authenticated attacker to bypass access restriction and access Network Maintenance page, which may result in obtaining the network information of the product. The affected products and versions are as follows: M2M Gateway with the firmware Ver.3.7.10 and earlier (CPS-MG341-ADSC1-111, CPS-MG341-ADSC1-931, CPS-MG341G-ADSC1-111, CPS-MG341G-ADSC1-930, and CPS-MG341G5-ADSC1-931), M2M Controller Integrated Type with firmware Ver.3.7.6 and earlier versions (CPS-MC341-ADSC1-111, CPS-MC341-ADSC1-931, CPS-MC341-ADSC2-111, CPS-MC341G-ADSC1-110, CPS-MC341Q-ADSC1-111, CPS-MC341-DS1-111, CPS-MC341-DS11-111, CPS-MC341-DS2-911, and CPS-MC341-A1-111), and M2M Controller Configurable Type with firmware Ver.3.8.8 and earlier versions (CPS-MCS341-DS1-111, CPS-MCS341-DS1-131, CPS-MCS341G-DS1-130, CPS-MCS341G5-DS1-130, and CPS-MCS341Q-DS1-131). | 4.3 | More Details |
| CVE-2023-1887 | Business Logic Errors in GitHub repository thorsten/phpmyfaq prior to 3.1.12. | 4.3 | More Details |
| CVE-2023-1903 | SAP HCM Fiori App My Forms (Fiori 2.0) - version 605, does not perform necessary authorization checks for an authenticated user exposing the restricted header data. | 4.3 | More Details |
| CVE-2022-35850 | An improper neutralization of script-related HTML tags in a web page vulnerability [CWE-80] in FortiAuthenticator versions 6.4.0 through 6.4.4, 6.3.0 through 6.3.3, all versions of 6.2 and 6.1 may allow a remote unauthenticated attacker to trigger a reflected cross site scripting (XSS) attack via the "reset-password" page. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1417 | An issue has been discovered in GitLab affecting all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible for an unauthorised user to add child epics linked to victim's epic in an unrelated group. | 4.3 | More Details |
| CVE-2013-10025 | A vulnerability was found in Exit Strategy Plugin 1.55 on WordPress and classified as problematic. Affected by this issue is the function exitpageadmin of the file exitpage.php. The manipulation leads to cross-site request forgery. The attack may be launched remotely. Upgrading to version 1.59 is able to address this issue. The patch is identified as d964b8e961b2634158719f3328f16eda16ce93ac. It is recommended to upgrade the affected component. VDB-225266 is the identifier assigned to this vulnerability. | 4.3 | More Details |
| CVE-2012-10010 | A vulnerability was found in BestWebSoft Contact Form 3.21. It has been classified as problematic. This affects the function cntctfrm_settings_page of the file contact_form.php. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 3.22 is able to address this issue. The identifier of the patch is 8398d96ff0fe45ec9267d7259961c2ef89ed8005. It is recommended to upgrade the affected component. The identifier VDB-225321 was assigned to this vulnerability. | 4.3 | More Details |
| CVE-2023-1926 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the deleteCacheToolbar function. This makes it possible for unauthenticated attackers to perform cache deletion via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1925 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_clear_cache_of_allsites_callback function. This makes it possible for unauthenticated attackers to clear caches via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-26845 | A Cross-Site Request Forgery (CSRF) in OpenCATS 0.9.7 allows attackers to force users into submitting web requests via unspecified vectors. | 4.3 | More Details |
| CVE-2023-1937 | A vulnerability, which was classified as problematic, was found in zhenfeng13 My-Blog. Affected is an unknown function of the file /admin/configurations/userInfo. The manipulation of the argument yourAvatar/yourName/yourEmail leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-225264. | 4.3 | More Details |
| CVE-2023-1924 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_toolbar_save_settings_callback function. This makes it possible for unauthenticated attackers to change cache settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1923 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_remove_cdn_integration_ajax_request_callback function. This makes it possible for unauthenticated attackers to change cdn settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1922 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_pause_cdn_integration_ajax_request_callback function. This makes it possible for unauthenticated attackers to change cdn settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1921 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_start_cdn_integration_ajax_request_callback function. This makes it possible for unauthenticated attackers to change cdn settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1939 | No access control for the OTP key on OTP entries in Devolutions Remote Desktop Manager Windows 2022.3.33.0 and prior versions and Remote Desktop Manager Linux 2022.3.2.0 and prior versions allows non admin users to see OTP keys via the user interface. | 4.3 | More Details |
| CVE-2023-0944 | Bhima version 1.27.0 allows an authenticated attacker with regular user permissions to update arbitrary user session data such as username, email and password. This is possible because the application is vulnerable to IDOR, it does not correctly validate user permissions with respect to certain actions that can be performed by the user. | 4.3 | More Details |
| CVE-2012-10012 | A vulnerability has been found in BestWebSoft Facebook Like Button up to 2.13 and classified as problematic. Affected by this vulnerability is the function fcbk_bttn_plgn_settings_page of the file facebook-button-plugin.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The patch is named 33144ae5a45ed07efe7fceca901d91365fdbf7cb. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-225355. | 4.3 | More Details |
| CVE-2023-1920 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_purgecache_varnish_callback function. This makes it possible for unauthenticated attackers to purge the varnish cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1787 | An issue has been discovered in GitLab affecting all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. A search timeout could be triggered if a specific HTML payload was used in the issue description. | 4.3 | More Details |
| CVE-2022-42469 | A permissive list of allowed inputs vulnerability [CWE-183] in FortiGate version 7.2.3 and below, version 7.0.9 and below Policy-based NGFW Mode may allow an authenticated SSL-VPN user to bypass the policy via bookmarks in the web portal. | 4.3 | More Details |
| CVE-2023-30450 | rpk in Redpanda before 23.1.2 mishandles the redpanda.rpc_server_tls field, leading to (for example) situations in which there is a data type mismatch that cannot be automatically fixed by rpk, and instead a user must reconfigure (while a cluster is turned off) in order to have TLS on broker RPC ports. NOTE: the fix was also backported to the 22.2 and 22.3 branches. | 4.3 | More Details |
| CVE-2023-21729 | Remote Procedure Call Runtime Information Disclosure Vulnerability | 4.3 | More Details |
| CVE-2023-1928 | The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the wpfc_preload_single_callback function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to initiate cache creation. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1919 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_preload_single_save_settings_callback function. This makes it possible for unauthenticated attackers to change cache-related settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1918 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_preload_single_callback function. This makes it possible for unauthenticated attackers to invoke a cache building action via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1927 | The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the deleteCssAndJsCacheToolbar function. This makes it possible for unauthenticated attackers to perform cache deletion via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 4.3 | More Details |
| CVE-2023-1929 | The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the wpfc_purgecache_varnish_callback function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to purge the varnish cache. | 4.3 | More Details |
| CVE-2023-25411 | Aten PE8108 2.4.232 is vulnerable to Cross Site Request Forgery (CSRF). | 4.3 | More Details |
| CVE-2014-125098 | A vulnerability was found in Dart http_server up to 0.9.5 and classified as problematic. Affected by this issue is the function VirtualDirectory of the file lib/src/virtual_directory.dart of the component Directory Listing Handler. The manipulation of the argument request.uri.path leads to cross site scripting. The attack may be launched remotely. Upgrading to version 0.9.6 is able to address this issue. The name of the patch is 27c1cbd8125bb0369e675eb72e48218496e48ffb. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-225356. | 4.3 | More Details |
| CVE-2023-1930 | The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data deletion due to a missing capability check on the wpfc_clear_cache_of_allsites_callback function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to delete caches. | 4.3 | More Details |
| CVE-2023-1931 | The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check on the deleteCssAndJsCacheToolbar function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to perform cache deletion. | 4.3 | More Details |
| CVE-2023-22641 | A url redirection to untrusted site ('open redirect') in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.9, FortiOS versions 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specially crafted requests. | 4.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-29110 | The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. | 3.7 | More Details |
| CVE-2023-29112 | The SAP Application Interface (Message Monitoring) - versions 600, 700, allows an authorized attacker to input links or headings with custom CSS classes into a comment. The comment will render links and custom CSS classes as HTML objects. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. | 3.7 | More Details |
| CVE-2020-9009 | The ShipStation.com plugin 1.1 and earlier for CS-Cart allows remote attackers to insert arbitrary information into the database (via action=shipnotify) because access to this endpoint is completely unchecked. The attacker must guess an order number. | 3.7 | More Details |
| CVE-2023-28301 | Microsoft Edge (Chromium-based) Tampering Vulnerability | 3.7 | More Details |
| CVE-2023-0450 | An issue has been discovered in GitLab affecting all versions starting from 8.1 to 15.8.5, and from 15.9 to 15.9.4, and from 15.10 to 15.10.1. It was possible to add a branch with an ambiguous name that could be used to social engineer users. | 3.7 | More Details |
| CVE-2023-1860 | A vulnerability was found in Keysight IXIA Hawkeye 3.3.16.28. It has been declared as problematic. This vulnerability affects unknown code of the file /licenses. The manipulation of the argument view with the input teste"><script>alert(%27c4ng4c3ir0%27)</script> leads to cross site scripting. The attack can be initiated remotely. VDB-224998 is the identifier assigned to this vulnerability. NOTE: Vendor did not respond if and how they may handle this issue. | 3.5 | More Details |
| CVE-2009-10004 | A vulnerability was found in Turante Sandbox Theme up to 1.5.2. It has been classified as problematic. This affects the function sandbox_body_class of the file functions.php. The manipulation of the argument page leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.6.1 is able to address this issue. The identifier of the patch is 8045b1e10970342f558b2c5f360e0bd135af2b10. It is recommended to upgrade the affected component. The identifier VDB-225357 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2023-1853 | A vulnerability, which was classified as problematic, has been found in SourceCodester Online Payroll System 1.0. This issue affects some unknown processing of the file /admin/employee_edit.php. The manipulation of the argument of leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224993 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2023-1852 | A vulnerability classified as problematic was found in SourceCodester Online Payroll System 1.0. This vulnerability affects unknown code of the file /admin/deduction_edit.php. The manipulation of the argument description leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-224992. | 3.5 | More Details |
| CVE-2023-1851 | A vulnerability classified as problematic has been found in SourceCodester Online Payroll System 1.0. This affects an unknown part of the file /admin/employee_add.php. The manipulation of the argument of 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-224991. | 3.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2022-43952 | An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiADC version 7.1.1 and below, version 7.0.3 and below, version 6.2.5 and below may allow an authenticated attacker to perform a cross-site scripting attack via crafted HTTP requests. | 3.5 | More Details |
| CVE-2014-125096 | A vulnerability was found in Fancy Gallery Plugin 1.5.12 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file class.options.php of the component Options Page. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.5.13 is able to address this issue. The identifier of the patch is fdf1f9e5a1ec738900f962e69c6fa4ec6055ed8d. It is recommended to upgrade the affected component. The identifier VDB-225349 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2013-10024 | A vulnerability has been found in Exit Strategy Plugin 1.55 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the file exitpage.php. The manipulation leads to information disclosure. The attack can be launched remotely. Upgrading to version 1.59 is able to address this issue. The identifier of the patch is d964b8e961b2634158719f3328f16eda16ce93ac. It is recommended to upgrade the affected component. The identifier VDB-225265 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2013-10022 | A vulnerability, which was classified as problematic, has been found in BestWebSoft Contact Form Plugin 3.51 on WordPress. Affected by this issue is the function cntctfrm_display_form/cntctfrm_check_form of the file contact_form.php. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 3.52 is able to address this issue. The patch is identified as 642ef1dc1751ab6642ce981fe126325bb574f898. It is recommended to upgrade the affected component. VDB-225002 is the identifier assigned to this vulnerability. | 3.5 | More Details |
| CVE-2018-25084 | A vulnerability, which was classified as problematic, has been found in Ping Identity Self-Service Account Manager 1.1.2. Affected by this issue is some unknown functionality of the file src/main/java/com/unboundid/webapp/ssam/SSAMController.java. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.1.3 is able to address this issue. The patch is identified as f64b10d63bb19ca2228b0c2d561a1a6e5a3bf251. It is recommended to upgrade the affected component. VDB-225362 is the identifier assigned to this vulnerability. | 3.5 | More Details |
| CVE-2014-125094 | A vulnerability classified as problematic was found in phpMiniAdmin up to 1.8.120510. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.9.140405 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-225001 was assigned to this vulnerability. | 3.5 | More Details |
| CVE-2014-125097 | A vulnerability, which was classified as problematic, was found in BestWebSoft Facebook Like Button up to 2.33. Affected is the function fcbkbttn_settings_page of the file facebook-button-plugin.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 2.34 is able to address this issue. The patch is identified as b766da8fa100779409a953f0e46c2a2448cbe99c. It is recommended to upgrade the affected component. VDB-225354 is the identifier assigned to this vulnerability. | 3.5 | More Details |
| CVE-2023-1988 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/?page=maintenance/brand. The manipulation of the argument Brand Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225536. | 3.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-1948 | A vulnerability, which was classified as problematic, has been found in PHPGurukul BP Monitoring Management System 1.0. This issue affects some unknown processing of the file add-family-member.php of the component Add New Family Member Handler. The manipulation of the argument Member Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225335. | 3.5 | More Details |
| CVE-2015-10098 | A vulnerability was found in Broken Link Checker Plugin up to 1.10.5 on WordPress. It has been rated as problematic. Affected by this issue is the function print_module_list/show_warnings_section_notice/status_text/ui_get_action_links. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.10.6 is able to address this issue. The name of the patch is f30638869e281461b87548e40b517738b4350e47. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-225152. | 3.5 | More Details |
| CVE-2014-125095 | A vulnerability was found in BestWebSoft Contact Form Plugin 1.3.4 on WordPress and classified as problematic. Affected by this issue is the function bws_add_menu_render of the file bws_menu/bws_menu.php. The manipulation of the argument bwsmn_form_email leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.3.7 is able to address this issue. The name of the patch is 4d531f74b4a801c805dc80360d4ea1312e9a278f. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-225320. | 3.5 | More Details |
| CVE-2023-28633 | GLPI is a free asset and IT management software package. Starting in version 0.84 and prior to versions 9.5.13 and 10.0.7, usage of RSS feeds is subject to server-side request forgery (SSRF). In case the remote address is not a valid RSS feed, an RSS autodiscovery feature is triggered. This feature does not check safety or URLs. Versions 9.5.13 and 10.0.7 contain a patch for this issue. | 3.5 | More Details |
| CVE-2023-22808 | An issue was discovered in the Arm Android Gralloc Module. A non-privileged user can read a small portion of the allocator process memory. This affects Bifrost r24p0 through r41p0 before r42p0, Valhall r24p0 through r41p0 before r42p0, and Avalon r41p0 before r42p0. | 3.3 | More Details |
| CVE-2022-46781 | An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU memory processing operations to access a limited amount outside of buffer bounds. This affects Valhall r29p0 through r41p0 before r42p0 and Avalon r41p0 before r42p0. | 3.3 | More Details |
| CVE-2023-26083 | Memory leak vulnerability in Mali GPU Kernel Driver in Midgard GPU Kernel Driver all versions from r6p0 - r32p0, Bifrost GPU Kernel Driver all versions from r0p0 - r42p0, Valhall GPU Kernel Driver all versions from r19p0 - r42p0, and Avalon GPU Kernel Driver all versions from r41p0 - r42p0 allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata. | 3.3 | More Details |
| CVE-2022-46396 | An issue was discovered in the Arm Mali Kernel Driver. A non-privileged user can make improper GPU memory processing operations to access a limited amount outside of buffer bounds. This affects Valhall r29p0 through r41p0 before r42p0 and Avalon r41p0 before r42p0. | 3.3 | More Details |
| CVE-2022-3375 | An issue has been discovered in GitLab affecting all versions starting from 11.10 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible to disclose the branch names when attacker has a fork of a project that was switched to private. | 3.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2023-29111 | The SAP AIF (ODATA service) - versions 755, 756, discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an attacker can cause a low impact on the confidentiality of the application. | 3.1 | More Details |
| CVE-2023-1071 | An issue has been discovered in GitLab affecting all versions from 15.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. Due to improper permissions checks it was possible for an unauthorised user to remove an issue from an epic. | 3.1 | More Details |
| CVE-2023-29192 | SilverwareGames.io versions before 1.2.19 allow users with access to the game upload panel to edit download links for games uploaded by other developers. This has been fixed in version 1.2.19. | 2.7 | More Details |
| CVE-2022-32871 | A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16. A person with physical access to a device may be able to use Siri to access private calendar information | 2.4 | More Details |
| CVE-2023-1946 | A vulnerability was found in SourceCodester Survey Application System 1.0 and classified as problematic. This issue affects some unknown processing of the component Add New Handler. The manipulation of the argument Title with the input <script>prompt(document.domain)</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225329 was assigned to this vulnerability. | 2.4 | More Details |
| CVE-2022-46717 | A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16.2 and iPadOS 16.2. A user with physical access to a locked Apple Watch may be able to view user photos via accessibility features | 2.4 | More Details |
| CVE-2023-1857 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/?page=product/manage_product&id=2. The manipulation of the argument Product Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224996. | 2.4 | More Details |
| CVE-2023-1961 | A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/?page=system_info. The manipulation of the argument System Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225348. | 2.4 | More Details |
| CVE-2023-1876 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none. | N/A | More Details |