SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 September 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-2023-1523	Using the TIOCLINUX ioctl request, a malicious snap could inject contents into the input of the controlling terminal which could allow it to cause arbitrary commands to be executed outside of the snap sandbox after the snap exits. Graphical terminal emulators like xterm, gnome-terminal and others are not affected - this can only be exploited when snaps are run on a virtual console.	10.0	More Details
CVE-2023-3703	Proscend Advice ICR Series routers FW version 1.76 - CWE-1392: Use of Default Credentials	10.0	More Details
CVE-2023-39979	There is a vulnerability in MXsecurity versions prior to 1.0.1 that can be exploited to bypass authentication. A remote attacker might access the system if the web service authenticator has insufficient random values.	9.8	More Details
CVE-2023-28581	Memory corruption in WLAN Firmware while parsing receieved GTK Keys in GTK KDE.	9.8	More Details
CVE-2023-28562	Memory corruption while handling payloads from remote ESL.	9.8	More Details
CVE-2023-4614	This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/installation/setThumbnailRc endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user.	9.8	More Details
CVE-2023-4613	This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/settings/upload endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4744	A vulnerability was found in Tenda AC8 16.03.34.06_cn_TDC01. It has been declared as critical. Affected by this vulnerability is the function formSetDeviceName. The manipulation leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-238633 was assigned to this vulnerability.	9.8	More Details
CVE-2023-4596	The Forminator plugin for WordPress is vulnerable to arbitrary file uploads due to file type validation occurring after a file has been uploaded to the server in the upload_post_image() function in versions up to, and including, 1.24.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2023-40743	** UNSUPPORTED WHEN ASSIGNED ** When integrating Apache Axis 1.x in an application, it may not have been obvious that looking up a service through "ServiceFactory.getService" allows potentially dangerous lookup mechanisms such as LDAP. When passing untrusted input to this API method, this could expose the application to DoS, SSRF and even attacks leading to RCE. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. As a workaround, you may review your code to verify no untrusted or unsanitized input is passed to "ServiceFactory.getService", or by applying the patch from https://github.com/apache/axis-axis1-java/commit/7e66753427466590d6def0125e448d2791723210 . The Apache Axis project does not expect to create an Axis 1.x release fixing this problem, though contributors that would like to work towards this are welcome.	9.8	More Details
CVE-2023-40980	File Upload vulnerability in DWSurvey DWSurvey-OSS v.3.2.0 and before allows a remote attacker to execute arbitrary code via the saveimage method and savveFile in the action/UploadAction.java file.	9.8	More Details
CVE-2023-39631	An issue in LanChain-ai Langchain v.0.0.245 allows a remote attacker to execute arbitrary code via the evaluate function in the numexpr library.	9.8	More Details
CVE-2023-36328	Integer Overflow vulnerability in mp_grow in libtom libtommath before commit beba892bc0d4e4ded4d667ab1d2a94f4d75109a9, allows attackers to execute arbitrary code and cause a denial of service (DoS).	9.8	More Details
CVE-2023-36327	Integer Overflow vulnerability in RELIC before commit 421f2e91cf2ba42473d4d54daf24e295679e290e, allows attackers to execute arbitrary code and cause a denial of service in pos argument in bn_get_prime function.	9.8	More Details
CVE-2023-36326	Integer Overflow vulnerability in RELIC before commit 34580d840469361ba9b5f001361cad659687b9ab, allows attackers to execute arbitrary code, cause a denial of service, and escalate privileges when calling realloc function in bn_grow function.	9.8	More Details
CVE-2023-36187	Buffer Overflow vulnerability in NETGEAR R6400v2 before version 1.0.4.118, allows remote unauthenticated attackers to execute arbitrary code via crafted URL to httpd.	9.8	More Details
CVE-2023-41910	An issue was discovered in lldpd before 1.0.17. By crafting a CDP PDU packet with specific CDP_TLV_ADDRESSES TLVs, a malicious actor can remotely force the lldpd daemon to perform an out-of-bounds read on heap memory. This occurs in cdp_decode in daemon/protocols/cdp.c.	9.8	More Details
CVE-2023-36361	Audimexee v14.1.7 was discovered to contain a SQL injection vulnerability via the p_table_name parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41552	Tenda AC7 V1.0 V15.03.06.44 and Tenda AC9 V3.0 V15.03.06.42_multi were discovered to contain a stack overflow via parameter ssid at url /goform/fast_setting_wifi_set.	9.8	More Details
CVE-2023-4178	Authentication Bypass by Spoofing vulnerability in Neutron Neutron Smart VMS allows Authentication Bypass.This issue affects Neutron Smart VMS: before b1130.1.0.1.	9.8	More Details
CVE-2023-4310	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) versions 23.2.1 and 23.2.2 contain a command injection vulnerability which can be exploited through a malicious HTTP request. Successful exploitation of this vulnerability can allow an unauthenticated remote attacker to execute underlying operating system commands within the context of the site user. This issue is fixed in version 23.2.3.	9.8	More Details
CVE-2023-41508	A hard coded password in Super Store Finder v3.6 allows attackers to access the administration panel.	9.8	More Details
CVE-2023-39361	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a SQL injection discovered in graph_view.php. Since guest users can access graph_view.php without authentication by default, if guest users are being utilized in an enabled state, there could be the potential for significant damage. Attackers may exploit this vulnerability, and there may be possibilities for actions such as the usurpation of administrative privileges or remote code execution. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2023-41009	File Upload vulnerability in adlered bolo-solo v.2.6 allows a remote attacker to execute arbitrary code via a crafted script to the authorization field in the header.	9.8	More Details
CVE-2023-39654	abupy up to v0.4.0 was discovered to contain a SQL injection vulnerability via the component abupy.MarketBu.ABuSymbol.search_to_symbol_dict.	9.8	More Details
CVE-2023-4531	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mestav Software E-commerce Software allows SQL Injection.This issue affects E-commerce Software: before 20230901 .	9.8	More Details
CVE-2023-4034	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Digita Information Technology Smartrise Document Management System allows SQL Injection.This issue affects Smartrise Document Management System: before Hvl-2.0.	9.8	More Details
CVE-2023-41012	An issue in China Mobile Communications China Mobile Intelligent Home Gateway v.HG6543C4 allows a remote attacker to execute arbitrary code via the authentication mechanism.	9.8	More Details
CVE-2023-3616	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mava Software Hotel Management System allows SQL Injection.This issue affects Hotel Management System: before 2.0.	9.8	More Details
CVE-2023-39681	Cuppa CMS v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the email_outgoing parameter at /Configuration.php. This vulnerability is triggered via a crafted payload.	9.8	More Details
CVE-2023-35072	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Coyav Travel Proagent allows SQL Injection.This issue affects Proagent: before 20230904 .	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35068	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BMA Personnel Tracking System allows SQL Injection.This issue affects Personnel Tracking System: before 20230904.	9.8	More Details
CVE-2023-35065	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Osoft Paint Production Management allows SQL Injection.This issue affects Paint Production Management: before 2.1.	9.8	More Details
CVE-2023-3374	Incomplete List of Disallowed Inputs vulnerability in Unisign Bookreen allows Privilege Escalation.This issue affects Bookreen: before 3.0.0.	9.8	More Details
CVE-2023-36100	An issue was discovered in IceCMS version 2.0.1, allows attackers to escalate privileges and gain sensitive information via UserID parameter in api/User/ChangeUser.	9.8	More Details
CVE-2023-36076	SQL Injection vulnerability in smanga version 3.1.9 and earlier, allows remote attackers to execute arbitrary code and gain sensitive information via mediaId, mangaId, and userId parameters in php/history/add.php.	9.8	More Details
CVE-2020-22612	Installer RCE on settings file write in MyBB before 1.8.22.	9.8	More Details
CVE-2023-41560	Tenda AC9 V3.0 V15.03.06.42_multi was discovered to contain a stack overflow via parameter firewallEn at url /goform/SetFirewallCfg.	9.8	More Details
CVE-2023-40839	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin function 'sub_ADF3C' contains a command execution vulnerability. In the "formSetIptv" function, obtaining the "list" and "vlanId" fields, unfiltered passing these two fields as parameters to the "sub_ADF3C" function to execute commands.	9.8	More Details
CVE-2023-40838	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin function 'sub_3A1D0' contains a command execution vulnerability.	9.8	More Details
CVE-2023-40837	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin function 'sub_ADD50' contains a command execution vulnerability. In the "formSetIptv" function, obtaining the "list" and "vlanId" fields, unfiltered passing these two fields as parameters to the "sub_ADD50" function to execute commands.	9.8	More Details
CVE-2023-41563	Tenda AC9 V3.0 V15.03.06.42_multi and Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter mac at url /goform/GetParentControlInfo.	9.8	More Details
CVE-2023-41562	Tenda AC7 V1.0 V15.03.06.44, Tenda AC9 V3.0 V15.03.06.42_multi, and Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter time at url /goform/PowerSaveSet.	9.8	More Details
CVE-2023-41561	Tenda AC9 V3.0 V15.03.06.42_multi and Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter startIp and endIp at url /goform/SetPptpServerCfg.	9.8	More Details
CVE-2023-41559	Tenda AC7 V1.0 V15.03.06.44, Tenda AC9 V3.0 V15.03.06.42_multi, and Tenda AC5 V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter page at url /goform/NatStaticSetting.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41364	In tine through 2023.01.14.325, the sort parameter of the /index.php endpoint allows SQL Injection.	9.8	More Details
CVE-2023-41558	Tenda AC7 V1.0 V15.03.06.44 was discovered to contain a stack overflow via parameter timeZone at url /goform/SetSysTimeCfg.	9.8	More Details
CVE-2023-41557	Tenda AC7 V1.0 V15.03.06.44 and Tenda AC5 V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter entrys and mitInterface at url /goform/addressNat.	9.8	More Details
CVE-2023-41556	Tenda AC7 V1.0 V15.03.06.44, Tenda AC9 V3.0 V15.03.06.42_multi, and Tenda AC5 V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter list at url /goform/SetIpMacBind.	9.8	More Details
CVE-2023-41555	Tenda AC7 V1.0 V15.03.06.44 was discovered to contain a stack overflow via parameter security_5g at url /goform/WifiBasicSet.	9.8	More Details
CVE-2023-41554	Tenda AC9 V3.0 V15.03.06.42_multi was discovered to contain a stack overflow via parameter wpapsk_crypto at url /goform/WifiExtraSet.	9.8	More Details
CVE-2023-41553	Tenda AC9 V3.0 V15.03.06.42_multi and Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 were discovered to contain a stack overflow via parameter list at url /goform/SetStaticRouteCfg.	9.8	More Details
CVE-2023-40840	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function "fromGetWirelessRepeat."	9.8	More Details
CVE-2023-40841	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function "add_white_node,"	9.8	More Details
CVE-2023-40842	Tengda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function "R7WebsSecurityHandler."	9.8	More Details
CVE-2023-31714	Chitor-CMS before v1.1.2 was discovered to contain multiple SQL injection vulnerabilities.	9.8	More Details
CVE-2023-4696	Improper Access Control in GitHub repository usememos/memos prior to 0.13.2.	9.8	More Details
CVE-2023-41748	Remote command execution due to improper input validation. The following products are affected: Acronis Cloud Manager (Windows) before build 6.2.23089.203.	9.8	More Details
CVE-2023-41746	Remote command execution due to improper input validation. The following products are affected: Acronis Cloud Manager (Windows) before build 6.2.23089.203.	9.8	More Details
CVE-2023-41637	An arbitrary file upload vulnerability in the Carica immagine function of GruppoSCAI RealGimm 1.1.37p38 allows attackers to execute arbitrary code via uploading a crafted HTML file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41636	A SQL injection vulnerability in the Data Richiesta dal parameter of GruppoSCAI RealGimm v1.1.37p38 allows attackers to access the database and execute arbitrary commands via a crafted SQL query.	9.8	More Details
CVE-2023-40843	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function "sub_73004."	9.8	More Details
CVE-2023-3162	The Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.7.7. This is due to insufficient verification on the user being supplied during a Stripe checkout through the plugin. This allows unauthenticated attackers to log in as users who have orders, who are typically customers.	9.8	More Details
CVE-2023-40582	find-exec is a utility to discover available shell commands. Versions prior to 1.0.3 did not properly escape user input and are vulnerable to Command Injection via an attacker controlled parameter. As a result, attackers may run malicious shell commands in the context of the running process. This issue has been addressed in version 1.0.3. users are advised to upgrade. Users unable to upgrade should ensure that all input passed to find-exec comes from a trusted source.	9.8	More Details
CVE-2023-40848	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via the function "sub_7D858."	9.8	More Details
CVE-2023-40847	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via the function "initIpAddrInfo." In the function, it reads in a user-provided parameter, and the variable is passed to the function without any length check.	9.8	More Details
CVE-2023-40845	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function 'sub_34FD0.' In the function, it reads user provided parameters and passes variables to the function without any length checks.	9.8	More Details
CVE-2023-40844	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function 'formWifiBasicSet.'	9.8	More Details
CVE-2023-41507	Super Store Finder v3.6 was discovered to contain multiple SQL injection vulnerabilities in the store locator component via the products, distance, lat, and lng parameters.	9.8	More Details
CVE-2023-28801	An Improper Verification of Cryptographic Signature in the SAML authentication of the Zscaler Admin UI allows a Privilege Escalation.This issue affects Admin UI: from 6.2 before 6.2r.	9.6	More Details
CVE-2017-9453	BMC Server Automation before 8.9.01 patch 1 allows Process Spawner command execution because of authentication bypass.	9.0	More Details
CVE-2023-4299	Digi RealPort Protocol is vulnerable to a replay attack that may allow an attacker to bypass authentication to access connected equipment.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2023-39359	Cacti is an open source operational monitoring and fault management framework. An authenticated SQL injection vulnerability was discovered which allows authenticated users to perform privilege escalation and remote code execution. The vulnerability resides in the `graphs.php` file. When dealing with the cases of ajax_hosts and ajax_hosts_noany, if the `site_id` parameter is greater than 0, it is directly reflected in the WHERE clause of the SQL statement. This creates an SQL injection vulnerability. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2015-1391	Aruba AirWave before 8.0.7 allows bypass of a CSRF protection mechanism.	8.8	More Details
CVE-2023-4019	The Media from FTP WordPress plugin before 11.17 does not properly limit who can use the plugin, which may allow users with author+ privileges to move files around, like wp-config.php, which may lead to RCE in some cases.	8.8	More Details
CVE-2023-37221	7Twenty BOT - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').	8.8	More Details
CVE-2023-39448	Path traversal vulnerability in SHIRASAGI prior to v1.18.0 allows a remote authenticated attacker to alter or create arbitrary files on the server, resulting in arbitrary code execution.	8.8	More Details
CVE-2023-39369	StarTrinity Softswitch version 2023-02-16 - Multiple Reflected XSS (CWE-79)	8.8	More Details
CVE-2023-39370	StarTrinity Softswitch version 2023-02-16 - Persistent XSS (CWE-79)	8.8	More Details
CVE-2023-39371	StarTrinity Softswitch version 2023-02-16 - Open Redirect (CWE-601)	8.8	More Details
CVE-2023-39357	Cacti is an open source operational monitoring and fault management framework. A defect in the sql_save function was discovered. When the column type is numeric, the sql_save function directly utilizes user input. Many files and functions calling the sql_save function do not perform prior validation of user input, leading to the existence of multiple SQL injection vulnerabilities in Cacti. This allows authenticated users to exploit these SQL injection vulnerabilities to perform privilege escalation and remote code execution. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-39358	Cacti is an open source operational monitoring and fault management framework. An authenticated SQL injection vulnerability was discovered which allows authenticated users to perform privilege escalation and remote code execution. The vulnerability resides in the `reports_user.php` file. In `ajax_get_branches`, the `tree_id` parameter is passed to the `reports_get_branch_select` function without any validation. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-31175	An Execution with Unnecessary Privileges vulnerability in the Schweitzer Engineering Laboratories SEL-5037 SEL Grid Configurator could allow an attacker to run system commands with the highest level privilege on the system. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5037 SEL Grid Configurator: before 4.5.0.20.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40918	KnowStreaming 3.3.0 is vulnerable to Escalation of Privileges. Unauthorized users can create a new user with an admin role.	8.8	More Details
CVE-2023-41640	An improper error handling vulnerability in the component ErroreNonGestito.aspx of GruppoSCAI RealGimm 1.1.37p38 allows attackers to obtain sensitive technical information via a crafted SQL query.	8.8	More Details
CVE-2023-41638	An arbitrary file upload vulnerability in the Gestione Documentale module of GruppoSCAI RealGimm 1.1.37p38 allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2023-40970	Senayan Library Management Systems SLIMS 9 Bulian v 9.6.1 is vulnerable to SQL Injection via admin/modules/circulation/loan_rules.php.	8.8	More Details
CVE-2023-4746	A vulnerability classified as critical has been found in TOTOLINK N200RE V5 9.3.5u.6437_B20230519. This affects the function Validity_check. The manipulation leads to format string. It is possible to initiate the attack remotely. The root-cause of the vulnerability is a format string issue. But the impact is to bypass the validation which leads to to OS command injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-238635.	8.8	More Details
CVE-2023-3677	The WooCommerce PDF Invoice Builder plugin for WordPress is vulnerable to SQL Injection via the pageId parameter in versions up to, and including, 1.2.89 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for subscribers or higher to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-3636	The WP Project Manager plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.6.4 due to insufficient restriction on the 'save_users_map_name' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'usernames' parameter.	8.8	More Details
CVE-2023-41108	TEF portal 2023-07-17 is vulnerable to authenticated remote code execution.	8.8	More Details
CVE-2023-2229	The Quick Post Duplicator for WordPress is vulnerable to SQL Injection via the ‘post_id’ parameter in versions up to, and including, 2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-40595	In Splunk Enterprise versions lower than 8.2.12, 9.0.6, and 9.1.1, an attacker can execute a specially crafted query that they can then use to serialize untrusted data. The attacker can use the query to execute arbitrary code.	8.8	More Details
CVE-2023-4762	Type Confusion in V8 in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4763	Use after free in Networks in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2453	There is insufficient sanitization of tainted file names that are directly concatenated with a path that is subsequently passed to a ‘require_once’ statement. This allows arbitrary files with the ‘.php’ extension for which the absolute path is known to be included and executed. There are no known means in PHPFusion through which an attacker can upload and target a ‘.php’ file payload.	8.8	More Details
CVE-2022-41763	An issue was discovered in NOKIA AMS 9.7.05. Remote Code Execution exists via the debugger of the ipAddress variable. A remote user, authenticated to the AMS server, could inject code in the PING function. The privileges of the command executed depend on the user that runs the service.	8.8	More Details
CVE-2023-4697	Improper Privilege Management in GitHub repository usememos/memos prior to 0.13.2.	8.8	More Details
CVE-2023-4571	In Splunk IT Service Intelligence (ITSI) versions below below 4.13.3, 4.15.3, or 4.17.1, a malicious actor can inject American National Standards Institute (ANSI) escape codes into Splunk ITSI log files that, when a vulnerable terminal application reads them, can run malicious code in the vulnerable application. This attack requires a user to use a terminal application that translates ANSI escape codes to read the malicious log file locally in the vulnerable terminal. The vulnerability also requires additional user interaction to succeed. The vulnerability does not directly affect Splunk ITSI. The indirect impact on Splunk ITSI can vary significantly depending on the permissions in the vulnerable terminal application, as well as where and how the user reads the malicious log file. For example, users can copy the malicious file from Splunk ITSI and read it on their local machine.	8.6	More Details
CVE-2023-3489	The firmwaredownload command on Brocade Fabric OS v9.2.0 could log the FTP/SFTP/SCP server password in clear text in the SupportSave file when performing a downgrade from Fabric OS v9.2.0 to any earlier version of Fabric OS.	8.6	More Details
CVE-2023-40598	In Splunk Enterprise versions below 8.2.12, 9.0.6, and 9.1.1, an attacker can create an external lookup that calls a legacy internal function. The attacker can use this internal function to insert code into the Splunk platform installation directory. From there, a user can execute arbitrary code on the Splunk platform Instance.	8.5	More Details
CVE-2022-40534	Memory corruption due to improper validation of array index in Audio.	8.4	More Details
CVE-2022-33275	Memory corruption due to improper validation of array index in WLAN HAL when received lm_itemNum is out of range.	8.4	More Details
CVE-2023-33021	Memory corruption in Graphics while processing user packets for command submission.	8.4	More Details
CVE-2023-28538	Memory corruption in WIN Product while invoking WinAcpi update driver in the UEFI region.	8.4	More Details
CVE-2023-40592	In Splunk Enterprise versions below 9.1.1, 9.0.6, and 8.2.12, an attacker can craft a special web request that can result in reflected cross-site scripting (XSS) on the “/app/search/table” web endpoint. Exploitation of this vulnerability can lead to the execution of arbitrary commands on the Splunk platform instance.	8.4	More Details
CVE-2023-4587	An IDOR vulnerability has been found in ZKTeco ZEM800 product affecting version 6.60. This vulnerability allows a local attacker to obtain registered user backup files or device configuration files over a local network or through a VPN server.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41039	RestrictedPython is a restricted execution environment for Python to run untrusted code. Python's "format" functionality allows someone controlling the format string to "read" all objects accessible through recursive attribute lookup and subscription from objects he can access. This can lead to critical information disclosure. With `RestrictedPython`, the format functionality is available via the `format` and `format_map` methods of `str` (and `unicode`) (accessed either via the class or its instances) and via `string.Formatter`. All known versions of `RestrictedPython` are vulnerable. This issue has been addressed in commit `4134aedcff1` which has been included in the 5.4 and 6.2 releases. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.3	More Details
CVE-2023-41054	LibreY is a fork of LibreX, a framework-less and javascript-free privacy respecting meta search engine. LibreY is subject to a Server-Side Request Forgery (SSRF) vulnerability in the `image_proxy.php` file of LibreY before commit 8f9b9803f231e2954e5b49987a532d28fe50a627. This vulnerability allows remote attackers to use the server as a proxy to send HTTP GET requests to arbitrary targets and retrieve information in the internal network or conduct Denial-of-Service (DoS) attacks via the `url` parameter. Remote attackers can use the server as a proxy to send HTTP GET requests and retrieve information in the internal network. Remote attackers can also request the server to download large files or chain requests among multiple instances to reduce the performance of the server or even deny access from legitimate users. This issue has been addressed in https://github.com/Ahwxorg/LibreY/pull/31. LibreY hosters are advised to use the latest commit. There are no known workarounds for this vulnerability.	8.2	More Details
CVE-2023-34392	A Missing Authentication for Critical Function vulnerability in the Schweitzer Engineering Laboratories SEL-5037 SEL Grid Configurator could allow an attacker to run arbitrary commands on managed devices by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5037 SEL Grid Configurator: before 4.5.0.20.	8.2	More Details
CVE-2023-39372	StarTrinity Softswitch version 2023-02-16 - Multiple CSRF (CWE-352)	8.1	More Details
CVE-2023-4761	Out of bounds memory access in FedCM in Google Chrome prior to 116.0.5845.179 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2023-28543	A malformed DLC can trigger Memory Corruption in SNPE library due to out of bounds read, such as by loading an untrusted model (e.g. from a remote source).	8.1	More Details
CVE-2023-34998	An authentication bypass vulnerability exists in the OAS Engine functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted series of network requests can lead to arbitrary authentication. An attacker can sniff network traffic to trigger this vulnerability.	8.1	More Details
CVE-2023-31242	An authentication bypass vulnerability exists in the OAS Engine functionality of Open Automation Software OAS Platform v18.00.0072. A specially-crafted series of network requests can lead to arbitrary authentication. An attacker can send a sequence of requests to trigger this vulnerability.	8.1	More Details
CVE-2023-4695	Use of Predictable Algorithm in Random Number Generator in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	8.1	More Details
CVE-2023-31424	Brocade SANnav Web interface before Brocade SANnav v2.3.0 and v2.2.2a allows remote unauthenticated users to bypass web authentication and authorization.	8.1	More Details
CVE-2023-3297	In Ubuntu's accountsservice an unprivileged local attacker can trigger a use-after-free vulnerability in accountsservice by sending a D-Bus message to the accounts-daemon process.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28557	Memory corruption in WLAN HAL while processing command parameters from untrusted WMI payload.	7.8	More Details
CVE-2023-28549	Memory corruption in WLAN HAL while parsing Rx buffer in processing TLV payload.	7.8	More Details
CVE-2023-28558	Memory corruption in WLAN handler while processing PhyID in Tx status handler.	7.8	More Details
CVE-2023-28548	Memory corruption in WLAN HAL while processing Tx/Rx commands from QDART.	7.8	More Details
CVE-2023-38453	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-28560	Memory corruption in WLAN HAL while processing devIndex from untrusted WMI payload.	7.8	More Details
CVE-2023-38452	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-28559	Memory corruption in WLAN FW while processing command parameters from untrusted WMI payload.	7.8	More Details
CVE-2023-38451	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-28564	Memory corruption in WLAN HAL while passing command parameters through WMI interfaces.	7.8	More Details
CVE-2023-38450	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-38449	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-28565	Memory corruption in WLAN HAL while handling command streams through WMI interfaces.	7.8	More Details
CVE-2023-28567	Memory corruption in WLAN HAL while handling command through WMI interfaces.	7.8	More Details
CVE-2023-28573	Memory corruption in WLAN HAL while parsing WMI command parameters.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28544	Memory corruption in WLAN while sending transmit command from HLOS to UTF handlers.	7.8	More Details
CVE-2023-4735	Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.1847.	7.8	More Details
CVE-2023-38455	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-38460	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-4736	Untrusted Search Path in GitHub repository vim/vim prior to 9.0.1833.	7.8	More Details
CVE-2023-24674	Permissions vulnerability found in Bludit CMS v.4.0.0 allows local attackers to escalate privileges via the role:admin parameter.	7.8	More Details
CVE-2023-4738	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1848.	7.8	More Details
CVE-2023-38464	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2022-46869	Local privilege escalation during installation due to improper soft link handling. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40278.	7.8	More Details
CVE-2023-4733	Use After Free in GitHub repository vim/vim prior to 9.0.1840.	7.8	More Details
CVE-2023-4750	Use After Free in GitHub repository vim/vim prior to 9.0.1857.	7.8	More Details
CVE-2023-4752	Use After Free in GitHub repository vim/vim prior to 9.0.1858.	7.8	More Details
CVE-2023-28072	Dell Alienware Command Center, versions prior to 5.5.51.0, contain a deserialization of untrusted data vulnerability. A local malicious user could potentially send specially crafted requests to the .NET Remoting server to run arbitrary code on the system.	7.8	More Details
CVE-2023-41744	Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Agent (macOS) before build 30600, Acronis Cyber Protect 15 (macOS) before build 35979.	7.8	More Details
CVE-2023-41743	Local privilege escalation due to insecure driver communication port permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40278, Acronis Agent (Windows) before build 31637, Acronis Cyber Protect 15 (Windows) before build 35979.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38456	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-38443	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-39374	ForeScout NAC SecureConnector version 11.2 - CWE-427: Uncontrolled Search Path Element	7.8	More Details
CVE-2022-46868	Local privilege escalation during recovery due to improper soft link handling. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40173.	7.8	More Details
CVE-2022-45451	Local privilege escalation due to insecure driver communication port permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40173, Acronis Agent (Windows) before build 30600, Acronis Cyber Protect 15 (Windows) before build 30984.	7.8	More Details
CVE-2023-38459	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-4751	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1331.	7.8	More Details
CVE-2023-38458	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2023-21662	Memory corruption in Core Platform while printing the response buffer in log.	7.8	More Details
CVE-2023-4734	Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.1846.	7.8	More Details
CVE-2023-21664	Memory Corruption in Core Platform while printing the response buffer in log.	7.8	More Details
CVE-2023-4487	GE CIMPLICITY 2023 is by a process control vulnerability, which could allow a local attacker to insert malicious configuration files in the expected web server execution path to escalate privileges and gain full control of the HMI software.	7.8	More Details
CVE-2023-38444	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	7.8	More Details
CVE-2020-35593	BMC PATROL Agent through 20.08.00 allows local privilege escalation via vectors involving pconfig +RESTART -host.	7.8	More Details
CVE-2023-39139	An issue in Archive v3.3.7 allows attackers to execute a path traversal via extracting a crafted zip file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39138	An issue in ZIPFoundation v0.9.16 allows attackers to execute a path traversal via extracting a crafted zip file.	7.8	More Details
CVE-2023-39137	An issue in Archive v3.3.7 allows attackers to spoof zip filenames which can lead to inconsistent filename parsing.	7.8	More Details
CVE-2023-31132	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a privilege escalation vulnerability. A low-privileged OS user with access to a Windows host where Cacti is installed can create arbitrary PHP files in a web document directory. The user can then execute the PHP files under the security context of SYSTEM. This allows an attacker to escalate privilege from a normal user account to SYSTEM. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.8	More Details
CVE-2023-39135	An issue in Zip Swift v2.1.2 allows attackers to execute a path traversal attack via a crafted zip entry.	7.8	More Details
CVE-2023-40597	In Splunk Enterprise versions lower than 8.2.12, 9.0.6, and 9.1.1, an attacker can exploit an absolute path traversal to execute arbitrary code that is located on a separate disk.	7.8	More Details
CVE-2023-4781	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1873.	7.8	More Details
CVE-2023-31173	Use of Hard-coded Credentials vulnerability in Schweitzer Engineering Laboratories SEL-5037 SEL Grid Configurator on Windows allows Authentication Bypass. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5037 SEL Grid Configurator: before 4.5.0.20.	7.7	More Details
CVE-2023-41055	LibreY is a fork of LibreX, a framework-less and javascript-free privacy respecting meta search engine. LibreY is subject to a Server-Side Request Forgery (SSRF) vulnerability in the `engines/google/text.php` and `engines/duckduckgo/text.php` files in versions before commit be59098abd119cda70b15bf3faac596dfd39a744. This vulnerability allows remote attackers to request the server to send HTTP GET requests to arbitrary targets and conduct Denial-of-Service (DoS) attacks via the `wikipedia_language` cookie. Remote attackers can request the server to download large files to reduce the performance of the server or even deny access from legitimate users. This issue has been patched in https://github.com/Ahwxorg/LibreY/pull/9. LibreY hosters are advised to use the latest commit. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-34353	An authentication bypass vulnerability exists in the OAS Engine authentication functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted network sniffing can lead to decryption of sensitive information. An attacker can sniff network traffic to trigger this vulnerability.	7.5	More Details
CVE-2023-41539	phpjabbers Business Directory Script 3.2 is vulnerable to SQL Injection via the column parameter.	7.5	More Details
CVE-2023-40771	SQL injection vulnerability in DataEase v.1.18.9 allows a remote attacker to obtain sensitive information via a crafted string outside of the blacklist function.	7.5	More Details
CVE-2023-40968	Buffer Overflow vulnerability in hzeller timg v.1.5.1 and before allows a remote attacker to cause a denial of service via the 0x61200000045c address.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41049	@dcl/single-sign-on-client is an open source npm library which deals with single sign on authentication flows. Improper input validation in the `init` function allows arbitrary javascript to be executed using the `javascript:` prefix. This vulnerability has been patched on version `0.1.0`. Users are advised to upgrade. Users unable to upgrade should limit untrusted user input to the `init` function.	7.5	More Details
CVE-2023-3222	Vulnerability in the password recovery mechanism of Password Recovery plugin for Roundcube, in its 1.2 version, which could allow a remote attacker to change an existing user´s password by adding a 6-digit numeric token. An attacker could create an automatic script to test all possible values because the platform has no limit on the number of requests.	7.5	More Details
CVE-2023-33914	In NIA0 algorithm in Security Mode Command, there is a possible missing verification incorrect input. This could lead to remote information disclosure no additional execution privileges needed	7.5	More Details
CVE-2023-33915	In LTE protocol stack, there is a possible missing permission check. This could lead to remote information disclosure no additional execution privileges needed	7.5	More Details
CVE-2023-36088	Server Side Request Forgery (SSRF) vulnerability in NebulaGraph Studio version 3.7.0, allows remote attackers to gain sensitive information.	7.5	More Details
CVE-2023-41058	Parse Server is an open source backend server. In affected versions the Parse Cloud trigger `beforeFind` is not invoked in certain conditions of `Parse.Query`. This can pose a vulnerability for deployments where the `beforeFind` trigger is used as a security layer to modify the incoming query. The vulnerability has been fixed by refactoring the internal query pipeline for a more concise code structure and implementing a patch to ensure the `beforeFind` trigger is invoked. This fix was introduced in commit `be4c7e23c6` and has been included in releases 6.2.2 and 5.5.5. Users are advised to upgrade. Users unable to upgrade should make use of parse server's security layers to manage access levels with Class-Level Permissions and Object-Level Access Control that should be used instead of custom security layers in Cloud Code triggers.	7.5	More Details
CVE-2023-41317	The Apollo Router is a configurable, high-performance graph router written in Rust to run a federated supergraph that uses Apollo Federation 2. Affected versions are subject to a Denial-of-Service (DoS) type vulnerability which causes the Router to panic and terminate when GraphQL Subscriptions are enabled. It can be triggered when **all of the following conditions are met**: 1. Running Apollo Router v1.28.0, v1.28.1 or v1.29.0 ("impacted versions"); **and** 2. The Supergraph schema provided to the Router (either via Apollo Uplink or explicitly via other configuration) **has a `subscription` type** with root-fields defined; **and** 3. The YAML configuration provided to the Router **has subscriptions enabled** (they are _disabled_ by default), either by setting `enabled: true` _or_ by setting a valid `mode` within the `subscriptions` object (as seen in [subscriptions' documentation](https://www.apollographql.com/docs/router/executing-operations/subscription-support/#router-setup)); **and** 4. An [anonymous](https://spec.graphql.org/draft/#sec-Anonymous-Operation-Definitions) (i.e., un-named) `subscription` operation (e.g., `subscription { ... }`) is received by the Router If **all four** of these criteria are met, the impacted versions will panic and terminate. There is no data-privacy risk or sensitive-information exposure aspect to this vulnerability. This is fixed in Apollo Router v1.29.1. Users are advised to upgrade. Updating to v1.29.1 should be a clear and simple upgrade path for those running impacted versions. However, if Subscriptions are **not** necessary for your Graph – but are enabled via configuration — then disabling subscriptions is another option to mitigate the risk.	7.5	More Details
CVE-2023-41627	O-RAN Software Community ric-plt-lib-rmr v4.9.0 does not validate the source of the routing tables it receives, potentially allowing attackers to send forged routing tables to the device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21653	Transient DOS in Modem while processing RRC reconfiguration message.	7.5	More Details
CVE-2023-21646	Transient DOS in Modem while processing invalid System Information Block 1.	7.5	More Details
CVE-2023-4279	This User Activity Log WordPress plugin before 1.6.7 retrieves client IP addresses from potentially untrusted headers, allowing an attacker to manipulate its value. This may be used to hide the source of malicious traffic.	7.5	More Details
CVE-2023-4616	This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/thumbnail endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the current user.	7.5	More Details
CVE-2023-28366	The broker in Eclipse Mosquitto 1.3.2 through 2.x before 2.0.16 has a memory leak that can be abused remotely when a client sends many QoS 2 messages with duplicate message IDs, and fails to respond to PUBREC commands. This occurs because of mishandling of EAGAIN from the libc send function.	7.5	More Details
CVE-2023-41749	Sensitive information disclosure due to excessive collection of system information. The following products are affected: Acronis Agent (Windows) before build 32047, Acronis Cyber Protect 15 (Windows) before build 35979.	7.5	More Details
CVE-2023-4540	Improper Handling of Exceptional Conditions vulnerability in Daurnimator lua-http library allows Excessive Allocation and a denial of service (DoS) attack to be executed by sending a properly crafted request to the server. Such a request causes the program to enter an infinite loop. This issue affects lua-http: all versions before commit ddab283.	7.5	More Details
CVE-2023-41909	An issue was discovered in FRRouting FRR through 9.0. bgp_nlri_parse_flowspec in bgpd/bgp_flowspec.c processes malformed requests with no attributes, leading to a NULL pointer dereference.	7.5	More Details
CVE-2023-33020	Transient DOS in WLAN Host when an invalid channel (like channel out of range) is received in STA during CSA IE.	7.5	More Details
CVE-2023-33019	Transient DOS in WLAN Host while doing channel switch announcement (CSA), when a mobile station receives invalid channel in CSA IE.	7.5	More Details
CVE-2023-33016	Transient DOS in WLAN firmware while parsing MLO (multi-link operation).	7.5	More Details
CVE-2023-33015	Transient DOS in WLAN Firmware while interpreting MBSSID IE of a received beacon frame.	7.5	More Details
CVE-2023-28584	Transient DOS in WLAN Host when a mobile station receives invalid channel in CSA IE while doing channel switch announcement (CSA).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40239	Certain Lexmark devices (such as CS310) before 2023-08-25 allow XXE attacks, leading to information disclosure. The fixed firmware version is LW80.*.P246, i.e., '*' indicates that the full version specification varies across product model family, but firmware level P246 (or higher) is required to remediate the vulnerability.	7.5	More Details
CVE-2022-46527	ELSYS ERS 1.5 Sound v2.3.8 was discovered to contain a buffer overflow via the NFC data parser.	7.5	More Details
CVE-2023-39685	An issue in hjson-java up to v3.0.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted JSON string.	7.5	More Details
CVE-2023-4698	Improper Input Validation in GitHub repository usememos/memos prior to 0.13.2.	7.5	More Details
CVE-2023-4481	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When certain specific crafted BGP UPDATE messages are received over an established BGP session, one BGP session may be torn down with an UPDATE message error, or the issue may propagate beyond the local system which will remain non-impacted, but may affect one or more remote systems. This issue is exploitable remotely as the crafted UPDATE message can propagate through unaffected systems and intermediate BGP speakers. Continuous receipt of the crafted BGP UPDATE messages will create a sustained Denial of Service (DoS) condition for impacted devices. This issue affects eBGP and iBGP, in both IPv4 and IPv6 implementations. This issue requires a remote attacker to have at least one established BGP session. Improper Input Validation, Denial of Service vulnerability in Juniper Networks, Inc. Junos OS (BGP, rpd modules), Juniper Networks, Inc. Junos OS Evolved (BGP, rpd modules) allows Fuzzing.This issue affects Junos OS: * All versions before 20.4R3-S10, * from 21.1R1 through 21.*, * from 21.2 before 21.2R3-S5, * from 21.3 before 21.3R3-S5, * from 21.4 before 21.4R3-S7 (unaffected from 21.4R3-S5, affected from 21.4R3-S6) * from 22.1 before 22.1R3-S4, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S1, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2. Junos OS Evolved: * All versions before 20.4R3-S10-EVO, * from 21.2-EVO before 21.2R3-S7-EVO, * from 21.3-EVO before 21.3R3-S5-EVO, * from 21.4-EVO before 21.4R3-S5-EVO, * from 22.1-EVO before 22.1R3-S4-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S1-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	7.5	More Details
CVE-2023-39982	A vulnerability has been identified in MXsecurity versions prior to v1.0.1. The vulnerability may put the confidentiality and integrity of SSH communications at risk on the affected device. This vulnerability is attributed to a hard-coded SSH host key, which might facilitate man-in-the-middle attacks and enable the decryption of SSH traffic.	7.5	More Details
CVE-2023-4615	This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/download/updateFile endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the current user.	7.5	More Details
CVE-2023-39981	A vulnerability that allows for unauthorized access has been discovered in MXsecurity versions prior to v1.0.1. This vulnerability arises from inadequate authentication measures, potentially leading to the disclosure of device information by a remote attacker.	7.5	More Details
CVE-2023-41742	Excessive attack surface due to binding to an unrestricted IP address. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 30430, Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 35979.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41628	An issue in O-RAN Software Community E2 G-Release allows attackers to cause a Denial of Service (DoS) by incorrectly initiating the messaging procedure between the E2Node and E2Term components.	7.5	More Details
CVE-2023-39373	A Hyundai model (2017) - CWE-294: Authentication Bypass by Capture-replay.	7.4	More Details
CVE-2023-31174	A Cross-Site Request Forgery (CSRF) vulnerability in the Schweitzer Engineering Laboratories SEL-5037 SEL Grid Configurator could allow an attacker to embed instructions that could be executed by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5037 SEL Grid Configurator: before 4.5.0.20.	7.4	More Details
CVE-2023-34391	Insecure Inherited Permissions vulnerability in Schweitzer Engineering Laboratories SEL-5033 AcSELerator RTAC Software on Windows allows Leveraging/Manipulating Configuration File Search Paths. See Instruction Manual Appendix A [Cybersecurity] tag dated 20230522 for more details. This issue affects SEL-5033 AcSELerator RTAC Software: before 1.35.151.21000.	7.4	More Details
CVE-2023-40187	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions of the 3.x beta branch are subject to a Use-After-Free issue in the `avc420_ensure_buffer` and `avc444_ensure_buffer` functions. If the value of `piDstSize[x]` is 0, `ppYUVDstData[x]` will be freed. However, in this case `ppYUVDstData[x]` will not have been updated which leads to a Use-After-Free vulnerability. This issue has been addressed in version 3.0.0-beta3. Users of the 3.x beta releases are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2023-3136	The MailArchiver plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an email subject in versions up to, and including, 2.10.1 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 a user accesses an injected page.	7.2	More Details
CVE-2023-41738	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in Directory Domain Functionality in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote authenticated users to execute arbitrary commands via unspecified vectors.	7.2	More Details
CVE-2023-2188	The Colibri Page Builder for WordPress is vulnerable to SQL Injection via the ‘post_id’ parameter in versions up to, and including, 1.0.227 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2023-37220	Synel Terminals - CWE-494: Download of Code Without Integrity Check	7.2	More Details
CVE-2023-20820	In wlan service, there is a possible command injection due to improper input validation. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00244189; Issue ID: WCNCR00244189.	7.2	More Details
CVE-2015-2201	Aruba AirWave before 7.7.14.2 and 8.x before 8.0.7 allows VisualRF remote OS command execution and file disclosure by administrative users.	7.2	More Details
CVE-2023-3375	Unrestricted Upload of File with Dangerous Type vulnerability in Unisign Bookreen allows OS Command Injection.This issue affects Bookreen: before 3.0.0.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39362	Cacti is an open source operational monitoring and fault management framework. In Cacti 1.2.24, under certain conditions, an authenticated privileged user, can use a malicious string in the SNMP options of a Device, performing command injection and obtaining remote code execution on the underlying server. The `lib/snmp.php` file has a set of functions, with similar behavior, that accept in input some variables and place them into an `exec` call without a proper escape or validation. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details
CVE-2015-2202	Aruba AirWave before 7.7.14.2 and 8.x before 8.0.7 allows administrative users to escalate privileges to root on the underlying OS.	7.2	More Details
CVE-2023-34180	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in KAPlugins Google Fonts For WordPress plugin <= 3.0.0 versions.	7.1	More Details
CVE-2023-32801	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Composite Products plugin <= 8.7.5 versions.	7.1	More Details
CVE-2023-40214	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Vathemes Business Pro theme <= 1.10.4 versions.	7.1	More Details
CVE-2023-40205	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Pixelgrade PixTypes plugin <= 1.4.15 versions.	7.1	More Details
CVE-2023-39991	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Blindside Networks BigBlueButton plugin <= 3.0.0-beta.4 versions.	7.1	More Details
CVE-2023-34175	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in GrandSlambert Login Configurator plugin <= 2.1 versions.	7.1	More Details
CVE-2023-40196	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ImageRecycle ImageRecycle pdf & image compression plugin <= 3.1.11 versions.	7.1	More Details
CVE-2023-39992	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in vCita.Com Online Booking & Scheduling Calendar for WordPress by vcita plugin <= 4.3.2 versions.	7.1	More Details
CVE-2023-32296	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Kangu para WooCommerce plugin <= 2.2.9 versions.	7.1	More Details
CVE-2023-34176	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Chilexpress Chilexpress woo oficial plugin <= 1.2.9 versions.	7.1	More Details
CVE-2023-32597	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Video Gallery plugin <= 1.0.10 versions.	7.1	More Details
CVE-2023-25471	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Webcodin WCP OpenWeather plugin <= 2.5.0 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30485	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Solwin Infotech Responsive WordPress Slider – Avartan Slider Lite plugin <= 1.5.3 versions.	7.1	More Details
CVE-2023-33325	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.30.1 versions.	7.1	More Details
CVE-2023-33320	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Mohammad I. Okfie WP-Hijri plugin <= 1.5.1 versions.	7.1	More Details
CVE-2023-33317	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Returns and Warranty Requests plugin <= 2.1.6 versions.	7.1	More Details
CVE-2023-39980	A vulnerability that allows the unauthorized disclosure of authenticated information has been identified in MXsecurity versions prior to v1.0.1. This vulnerability arises when special elements are not neutralized correctly, allowing remote attackers to alter SQL commands.	7.1	More Details
CVE-2023-25019	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Premio Chaty plugin <= 3.0.9 versions	7.1	More Details
CVE-2023-34184	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Bhavik Patel Woocommerce Order address Print plugin <= 3.2 versions.	7.1	More Details
CVE-2023-37997	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Dharmesh Patel Post List With Featured Image plugin <= 1.2 versions.	7.1	More Details
CVE-2023-32802	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce WooCommerce Pre-Orders plugin <= 1.9.0 versions.	7.1	More Details
CVE-2023-37893	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Chop-Chop Coming Soon Chop Chop plugin <= 2.2.4 versions.	7.1	More Details
CVE-2023-34023	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Miled WordPress Social Login plugin <= 3.0.4 versions.	7.1	More Details
CVE-2023-34022	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Rakib Hasan Dynamic QR Code Generator plugin <= 0.0.5 versions.	7.1	More Details
CVE-2023-35892	IBM Financial Transaction Manager for SWIFT Services 3.2.4 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: 258786.	7.1	More Details
CVE-2023-34174	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in BBS e-Theme BBS e-Popup plugin <= 2.4.5 versions.	7.1	More Details
CVE-2023-39162	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in XLPlugins User Email Verification for WooCommerce plugin <= 3.5.0 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32742	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in VeronaLabs WP SMS plugin <= 6.1.4 versions.	7.1	More Details
CVE-2023-20900	A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .	7.1	More Details
CVE-2023-34032	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Pascal Casier bbPress Toolkit plugin <= 1.0.12 versions.	7.1	More Details
CVE-2023-25453	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ian Sadovy WordPress Tables plugin <= 1.3.9 versions.	7.1	More Details
CVE-2023-25466	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Mahlamusa Who Hit The Page – Hit Counter plugin <= 1.4.14.3 versions.	7.1	More Details
CVE-2023-40208	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Aleksandar Urošević Stock Ticker plugin <= 3.23.3 versions.	7.1	More Details
CVE-2023-34008	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in weDevs WP ERP plugin <= 1.12.3 versions.	7.1	More Details
CVE-2023-34011	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in ShopConstruct plugin <= 1.1.2 versions.	7.1	More Details
CVE-2023-39164	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Molongui Author Box for Authors, Co-Authors, Multiple Authors and Guest Authors – Molongui plugin <= 4.6.19 versions.	7.1	More Details
CVE-2023-30494	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ImageRecycle ImageRecycle pdf & image compression plugin <= 3.1.10 versions.	7.1	More Details
CVE-2023-31220	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WP-EXPERTS.IN TEAM WP Categories Widget plugin <= 2.2 versions.	7.1	More Details
CVE-2023-37393	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Atarim Visual Website Collaboration, Feedback & Project Management – Atarim plugin <= 3.9.3 versions.	7.1	More Details
CVE-2023-39918	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in SAASPROJECT Booking Package Booking Package plugin <= 1.6.01 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39355	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Versions of FreeRDP on the 3.x release branch before beta3 are subject to a Use-After-Free in processing `RDPGFX_CMDID_RESETGRAPHICS` packets. If `context->maxPlaneSize` is 0, `context->planesBuffer` will be freed. However, without updating `context->planesBuffer`, this leads to a Use-After-Free exploit vector. In most environments this should only result in a crash. This issue has been addressed in version 3.0.0-beta3 and users of the beta 3.x releases are advised to upgrade. There are no known workarounds for this vulnerability.	7.0	More Details
CVE-2023-40596	In Splunk Enterprise versions earlier than 8.2.12, 9.0.6, and 9.1.1, a dynamic link library (DLL) that ships with Splunk Enterprise references an insecure path for the OPENSSLDIR build definition. An attacker can abuse this reference and subsequently install malicious code to achieve privilege escalation on the Windows machine.	7.0	More Details
CVE-2023-32811	In connectivity system driver, 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: ALPS07929848; Issue ID: ALPS07929848.	6.7	More Details
CVE-2023-32812	In gnss service, there is a possible out of bounds write due to improper input validation. This could lead to local esclation of privileges with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017365; Issue ID: ALPS08017365.	6.7	More Details
CVE-2023-20821	In nvram, 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: ALPS07937113; Issue ID: ALPS07937113.	6.7	More Details
CVE-2023-32806	In wlan driver, 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: ALPS07441589; Issue ID: ALPS07441589.	6.7	More Details
CVE-2023-38553	In gnss service, 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	6.7	More Details
CVE-2023-21636	Memory Corruption due to improper validation of array index in Linux while updating adn record.	6.7	More Details
CVE-2023-21644	Memory corruption in RIL due to Integer Overflow while triggering qcril_uim_request_apdu request.	6.7	More Details
CVE-2023-20822	In netdagent, 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: ALPS07944012; Issue ID: ALPS07944012.	6.7	More Details
CVE-2023-21654	Memory corruption in Audio during playback session with audio effects enabled.	6.7	More Details
CVE-2023-21655	Memory corruption in Audio while validating and mapping metadata.	6.7	More Details
CVE-2023-20829	In gps, 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: ALPS08014144; Issue ID: ALPS08014148.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20830	In gps, 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: ALPS08014144; Issue ID: ALPS08014156.	6.7	More Details
CVE-2023-20831	In gps, 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: ALPS08014144; Issue ID: ALPS08014162.	6.7	More Details
CVE-2023-20832	In gps, 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: ALPS08014144; Issue ID: ALPS08013530.	6.7	More Details
CVE-2023-20828	In gps, 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: ALPS08014144; Issue ID: ALPS08014144.	6.7	More Details
CVE-2023-20837	In seninf, 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: ALPS07992786; Issue ID: ALPS07992786.	6.7	More Details
CVE-2022-40524	Memory corruption due to buffer over-read in Modem while processing SetNativeHandle RTP service.	6.7	More Details
CVE-2023-21663	Memory Corruption while accessing metadata in Display.	6.7	More Details
CVE-2023-37994	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Artem Abramovich Art Decoration Shortcode plugin <= 1.5.6 versions.	6.5	More Details
CVE-2023-20842	In imgsys_cmdq, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07354259; Issue ID: ALPS07340477.	6.5	More Details
CVE-2023-20850	In imgsys_cmdq, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07340381.	6.5	More Details
CVE-2023-20848	In imgsys_cmdq, there is a possible out of bounds read due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07340433.	6.5	More Details
CVE-2023-20849	In imgsys_cmdq, there is a possible use after free due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07340350.	6.5	More Details
CVE-2023-32805	In power, there is a possible out of bounds write due to an insecure default value. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08102892; Issue ID: ALPS08102892.	6.5	More Details
CVE-2023-20841	In imgsys, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326441.	6.5	More Details
CVE-2023-20840	In imgsys, there is a possible out of bounds read and write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326430; Issue ID: ALPS07326430.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38516	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WP OnlineSupport, Essential Plugin Audio Player with Playlist Ultimate plugin <= 1.2.2 versions.	6.5	More Details
CVE-2023-32578	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Twinpictures Column-Matic plugin <= 1.3.3 versions.	6.5	More Details
CVE-2023-3720	The Upload Media By URL WordPress plugin before 1.0.8 does not have CSRF check when uploading files, which could allow attackers to make logged in admins upload files (including HTML containing JS code for users with the unfiltered_html capability) on their behalf.	6.5	More Details
CVE-2023-40197	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Devaldi Ltd flowpaper plugin <= 1.9.9 versions.	6.5	More Details
CVE-2023-41635	A XML External Entity (XXE) vulnerability in the VerifichePeriodiche.aspx component of GruppoSCAI RealGimm v1.1.37p38 allows attackers to read any file in the filesystem via supplying a crafted XML file.	6.5	More Details
CVE-2023-34317	An improper input validation vulnerability exists in the OAS Engine User Creation functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted series of network requests can lead to unexpected data in the configuration. An attacker can send a sequence of requests to trigger this vulnerability.	6.5	More Details
CVE-2023-4013	The GDPR Cookie Compliance (CCPA, DSGVO, Cookie Consent) WordPress plugin before 4.12.5 does not have proper CSRF checks when managing its license, which could allow attackers to make logged in admins update and deactivate the plugin's license via CSRF attacks	6.5	More Details
CVE-2023-32615	A file write vulnerability exists in the OAS Engine configuration functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted series of network requests can lead to arbitrary file creation or overwrite. An attacker can send a sequence of requests to trigger this vulnerability.	6.5	More Details
CVE-2023-32271	An information disclosure vulnerability exists in the OAS Engine configuration management functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted series of network requests can lead to a disclosure of sensitive information. An attacker can send a sequence of requests to trigger this vulnerability.	6.5	More Details
CVE-2023-3915	An issue has been discovered in GitLab EE affecting all versions starting from 16.1 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. If an external user is given an owner role on any group, that external user may escalate their privileges on the instance by creating a service account in that group. This service account is not classified as external and may be used to access internal projects.	6.5	More Details
CVE-2023-41034	Eclipse Leshan is a device management server and client Java implementation. In affected versions DDFFileParser` and `DefaultDDFFileValidator` (and so `ObjectLoader`) are vulnerable to `XXE Attacks`. A DDF file is a LWM2M format used to store LWM2M object description. Leshan users are impacted only if they parse untrusted DDF files (e.g. if they let external users provide their own model), in that case they MUST upgrade to fixed version. If you parse only trusted DDF file and validate only with trusted xml schema, upgrading is not mandatory. This issue has been fixed in versions 1.5.0 and 2.0.0-M13. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-34004	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WooCommerce WooCommerce Box Office plugin <= 1.1.50 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35094	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Julien Berthelot / MPEmbed WP Matterport Shortcode plugin <= 2.1.4 versions.	6.5	More Details
CVE-2023-41747	Sensitive information disclosure due to unauthenticated path traversal. The following products are affected: Acronis Cloud Manager (Windows) before build 6.2.23089.203.	6.5	More Details
CVE-2023-32746	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WooCommerce WooCommerce Brands plugin <= 1.6.45 versions.	6.5	More Details
CVE-2023-20266	A vulnerability in Cisco Emergency Responder, Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an authenticated, remote attacker to elevate privileges to root on an affected device. This vulnerability exists because the application does not properly restrict the files that are being used for upgrades. An attacker could exploit this vulnerability by providing a crafted upgrade file. A successful exploit could allow the attacker to elevate privileges to root. To exploit this vulnerability, the attacker must have valid platform administrator credentials on an affected device.	6.5	More Details
CVE-2023-32793	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WooCommerce WooCommerce Pre-Orders plugin <= 2.0.0 versions.	6.5	More Details
CVE-2023-40594	In Splunk Enterprise versions lower than 8.2.12, 9.0.6, and 9.1.1, an attacker can use the `printf` SPL function to perform a denial of service (DoS) against the Splunk Enterprise instance.	6.5	More Details
CVE-2023-32102	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Pexle Chris Library Viewer plugin <= 2.0.6 versions.	6.5	More Details
CVE-2023-40186	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an IntegerOverflow leading to Out-Of-Bound Write Vulnerability in the `gdi_CreateSurface` function. This issue affects FreeRDP based clients only. FreeRDP proxies are not affected as image decoding is not done by a proxy. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2023-2173	The BadgeOS plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.7.1.6. This is due to improper validation and authorization checks within the badgeos_delete_step_ajax_handler, badgeos_delete_award_step_ajax_handler, badgeos_delete_deduct_step_ajax_handler, and badgeos_delete_rank_req_step_ajax_handler functions. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete arbitrary posts.	6.5	More Details
CVE-2023-40567	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Write in the `clear_decompress_bands_data` function in which there is no offset validation. Abuse of this vulnerability may lead to an out of bounds write. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. there are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-40569	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Write in the `progressive_decompress` function. This issue is likely down to incorrect calculations of the `nXSrc` and `nYSrc` variables. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. there are no known workarounds for this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40574	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Write in the `writePixelBGRX` function. This issue is likely down to incorrect calculations of the `nHeight` and `srcStep` variables. This issue has been addressed in version 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2023-4640	The controller responsible for setting the logging level does not include any authorization checks to ensure the user is authenticated. This can be seen by noting that it extends Controller rather than AuthenticatedController and includes no further checks. This issue affects YugabyteDB Anywhere: from 2.0.0 through 2.17.3	6.5	More Details
CVE-2023-39988	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in 标准云(std.Cloud) WxSync plugin <= 2.7.23 versions.	6.5	More Details
CVE-2023-4764	Incorrect security UI in BFCache in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2023-3205	An issue has been discovered in GitLab affecting all versions starting from 15.11 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. An authenticated user could trigger a denial of service when importing or cloning malicious content.	6.5	More Details
CVE-2023-3210	An issue has been discovered in GitLab affecting all versions starting from 15.11 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. An authenticated user could trigger a denial of service when importing or cloning malicious content.	6.5	More Details
CVE-2023-21667	Transient DOS in Bluetooth HOST while passing descriptor to validate the blacklisted BT keyboard.	6.5	More Details
CVE-2023-20834	In pda, 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: ALPS07608514; Issue ID: ALPS07608514.	6.4	More Details
CVE-2023-4718	The Font Awesome 4 Menus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fa' and 'fa-stack' shortcodes in versions up to, and including, 4.7.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4599	The Slimstat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'eeb_mailto' shortcode in versions up to, and including, 2.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4597	The Slimstat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slimstat' shortcode in versions up to, and including, 5.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-20827	In ims service, there is a possible memory corruption 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: ALPS07937105; Issue ID: ALPS07937105.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20835	In camsys, 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: ALPS07341261; Issue ID: ALPS07326570.	6.4	More Details
CVE-2023-41046	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible in XWiki to execute Velocity code without having script right by creating an XClass with a property of type "TextArea" and content type "VelocityCode" or "VelocityWiki". For the former, the syntax of the document needs to be set the `xwiki/1.0` (this syntax doesn't need to be installed). In both cases, when adding the property to an object, the Velocity code is executed regardless of the rights of the author of the property (edit right is still required, though). In both cases, the code is executed with the correct context author so no privileged APIs can be accessed. However, Velocity still grants access to otherwise inaccessible data and APIs that could allow further privilege escalation. At least for "VelocityCode", this behavior is most likely very old but only since XWiki 7.2, script right is a separate right, before that version all users were allowed to execute Velocity and thus this was expected and not a security issue. This has been patched in XWiki 14.10.10 and 15.4 RC1. Users are advised to upgrade. There are no known workarounds.	6.3	More Details
CVE-2023-4000	The Waiting: One-click countdowns plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 0.6.2. This is due to missing or incorrect nonce validation on its AJAX actions. This makes it possible for unauthenticated attackers to create and delete countdowns, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.3	More Details
CVE-2023-4739	A vulnerability, which was classified as critical, has been found in Byzoro Smart S85F Management Platform up to 20230820. Affected by this issue is some unknown functionality of the file /sysmanage/updateos.php. The manipulation of the argument 1_file_upload leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-238628. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4740	A vulnerability, which was classified as critical, was found in IBOS OA 4.5.5. This affects an unknown part of the file ?r=email/api/delDraft&archiveId=0 of the component Delete Draft Handler. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-238629 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4741	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. This vulnerability affects unknown code of the file ?r=diary/default/del of the component Delete Logs Handler. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-238630 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4742	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. This issue affects some unknown processing of the file ?r=dashboard/user/export&uid=X. The manipulation 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-238631. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-40593	In Splunk Enterprise versions lower than 9.0.6 and 8.2.12, a malicious actor can send a malformed security assertion markup language (SAML) request to the `/saml/acs` REST endpoint which can cause a denial of service through a crash or hang of the Splunk daemon.	6.3	More Details
CVE-2023-20851	In stc, there is a possible out of bounds read due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08048635; Issue ID: ALPS08048635.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4745	A vulnerability was found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230822. It has been rated as critical. Affected by this issue is some unknown functionality of the file /importexport.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-238634 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4747	A vulnerability classified as critical was found in DedeCMS 5.7.110. This vulnerability affects unknown code of the file /uploads/tags.php. The manipulation of the argument tag_alias 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-238636.	6.3	More Details
CVE-2023-4749	A vulnerability, which was classified as critical, was found in SourceCodester Inventory Management System 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument page leads to file inclusion. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-238638 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4748	A vulnerability, which was classified as critical, has been found in Yongyou UFIDA-NC up to 20230807. This issue affects some unknown processing of the file PrintTemplateFileServlet.java. The manipulation of the argument filePath leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-238637 was assigned to this vulnerability.	6.3	More Details
CVE-2023-4708	A vulnerability was found in Infosoftbd Clcknshop 1.0.0. It has been rated as critical. This issue affects some unknown processing of the file /collection/all of the component GET Parameter Handler. The manipulation of the argument tag leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-238571. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3999	The Waiting: One-click countdowns plugin for WordPress is vulnerable to authorization bypass due to missing capability checks on its AJAX calls in versions up to, and including, 0.6.2. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to create and delete countdowns as well as manipulate other plugin settings.	6.3	More Details
CVE-2023-39514	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `graphs.php` displays graph details such as data-source paths, data template information and graph related fields. _CENSUS_ found that an adversary that is able to configure either a data-source template with malicious code appended in the data-source name or a device with a malicious payload injected in the device name, may deploy a stored XSS attack against any user with _General Administration>Graphs_ privileges. A user that possesses the _Template Editor>Data Templates_ permissions can configure the data-source name in _cacti_. Please note that this may be a _low privileged_ user. This configuration occurs through `http://<HOST>/cacti/data_templates.php` by editing an existing or adding a new data template. If a template is linked to a graph then the formatted template name will be rendered in the graph's management page. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device name in _cacti_. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to upgrade should add manual HTML escaping.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39516	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `data_sources.php` displays the data source management information (e.g. data source path, polling configuration etc.) for different data visualizations of the _cacti_ app. CENSUS found that an adversary that is able to configure a malicious data-source path, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the 'General Administration>Sites/Devices/Data' permissions can configure the data source path in Cacti. This configuration occurs through `http://<HOST>/cacti/data_sources.php`. The same page can be used for previewing the data source path. This issue has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to upgrade should manually escape HTML output.	6.1	More Details
CVE-2023-39515	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data stored in the cacti's database. These data will be viewed by administrative cacti accounts and execute JavaScript code in the victim's browser at view-time. The script under `data_debug.php` displays data source related debugging information such as _data source paths, polling settings, meta-data on the data source_. _CENSUS_ found that an adversary that is able to configure a malicious data-source path, can deploy a stored XSS attack against any user that has privileges related to viewing the `data_debug.php` information. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the data source path in _cacti_. This configuration occurs through `http://<HOST>/cacti/data_sources.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	6.1	More Details
CVE-2023-38574	Open redirect vulnerability in VI Web Client prior to 7.9.6 allows a remote unauthenticated attacker to redirect users to arbitrary web sites and conduct phishing attacks via a specially crafted URL.	6.1	More Details
CVE-2023-39513	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `host.php` is used to monitor and manage hosts in the _cacti_ app, hence displays useful information such as data queries and verbose logs. _CENSUS_ found that an adversary that is able to configure a data-query template with malicious code appended in the template path, in order to deploy a stored XSS attack against any user with the _General Administration>Sites/Devices/Data_ privileges. A user that possesses the _Template Editor>Data Queries_ permissions can configure the data query template path in _cacti_. Please note that such a user may be a low privileged user. This configuration occurs through `http://<HOST>/cacti/data_queries.php` by editing an existing or adding a new data query template. If a template is linked to a device then the formatted template path will be rendered in the device's management page, when a _verbose data query_ is requested. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	6.1	More Details
CVE-2023-39598	Cross Site Scripting vulnerability in IceWarp Corporation WebClient v.10.2.1 allows a remote attacker to execute arbitrary code via a crafted payload to the mid parameter.	6.1	More Details
CVE-2023-41538	phpjabbers PHP Forum Script 3.0 is vulnerable to Cross Site Scripting (XSS) via the keyword parameter.	6.1	More Details
CVE-2023-4151	The Store Locator WordPress plugin before 1.4.13 does not sanitise and escape an invalid nonce before outputting it back in an AJAX response, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4284	The Post Timeline WordPress plugin before 2.2.6 does not sanitise and escape an invalid nonce before outputting it back in an AJAX response, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-39366	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The `data_sources.php` script displays the data source management information (e.g. data source path, polling configuration etc.) for different data visualizations of the _cacti_ app. CENSUS found that an adversary that is able to configure a malicious Device name, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/data_sources.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	6.1	More Details
CVE-2023-39360	Cacti is an open source operational monitoring and fault management framework.Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data. The vulnerability is found in `graphs_new.php`. Several validations are performed, but the `returnto` parameter is directly passed to `form_save_button`. In order to bypass this validation, returnto must contain `host.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	6.1	More Details
CVE-2023-3992	The PostX WordPress plugin before 3.0.6 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	6.1	More Details
CVE-2023-41642	Multiple reflected cross-site scripting (XSS) vulnerabilities in the ErroreNonGestito.aspx component of GruppoSCAI RealGimm 1.1.37p38 allow attackers to execute arbitrary Javascript in the context of a victim user's browser via a crafted payload injected into the VIEWSTATE parameter.	6.1	More Details
CVE-2023-39714	Multiple cross-site scripting (XSS) vulnerabilities in Free and Open Source Inventory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name, Address, and Company parameters under the Add New Member section.	6.1	More Details
CVE-2015-1390	Aruba AirWave before 8.0.7 allows XSS attacks agsinat an administrator.	6.1	More Details
CVE-2023-4471	The Order Tracking Pro plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the start_date and end_date parameters in versions up to, and including, 3.3.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-4315	The Woo Custom Emails for WordPress is vulnerable to Reflected Cross-Site Scripting via the wcemails_edit parameter in versions up to, and including, 2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-4655	Cross-site Scripting (XSS) - Reflected in GitHub repository instantsoft/icms2 prior to 2.16.1.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36492	Reflected cross-site scripting vulnerability in SHIRASAGI prior to v1.18.0 allows a remote unauthenticated attacker to execute an arbitrary script on the web browser of the user who is logging in to the product.	6.1	More Details
CVE-2023-39938	Reflected cross-site scripting vulnerability in VI Web Client prior to 7.9.6 allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2023-2813	All of the above Aapna WordPress theme through 1.3, Anand WordPress theme through 1.2, Anfaust WordPress theme through 1.1, Arendelle WordPress theme before 1.1.13, Atlast Business WordPress theme through 1.5.8.5, Bazaar Lite WordPress theme before 1.8.6, Brain Power WordPress theme through 1.2, BunnyPressLite WordPress theme before 2.1, Cafe Bistro WordPress theme before 1.1.4, College WordPress theme before 1.5.1, Connections Reloaded WordPress theme through 3.1, Counterpoint WordPress theme through 1.8.1, Digitally WordPress theme through 1.0.8, Directory WordPress theme before 3.0.2, Drop WordPress theme before 1.22, Everse WordPress theme before 1.2.4, Fashionable Store WordPress theme through 1.3.4, Fullbase WordPress theme before 1.2.1, Ilex WordPress theme before 1.4.2, Js O3 Lite WordPress theme through 1.5.8.2, Js Paper WordPress theme through 2.5.7, Kata WordPress theme before 1.2.9, Kata App WordPress theme through 1.0.5, Kata Business WordPress theme through 1.0.2, Looki Lite WordPress theme before 1.3.0, moseter WordPress theme through 1.3.1, Nokke WordPress theme before 1.2.4, Nothing Personal WordPress theme through 1.0.7, Offset Writing WordPress theme through 1.2, Opor Ayam WordPress theme through 18, Pinzolo WordPress theme before 1.2.10, Plato WordPress theme before 1.1.9, Polka Dots WordPress theme through 1.2, Purity Of Soul WordPress theme through 1.9, Restaurant PT WordPress theme before 1.1.3, Saul WordPress theme before 1.1.0, Sean Lite WordPress theme before 1.4.6, Tantyyellow WordPress theme through 1.0.0.5, TIJAJI WordPress theme through 1.43, Tiki Time WordPress theme through 1.3, Tuaug4 WordPress theme through 1.4, Tydskrif WordPress theme through 1.1.3, UltraLight WordPress theme through 1.2, Venice Lite WordPress theme before 1.5.5, Viala WordPress theme through 1.3.1, viburno WordPress theme before 1.3.2, Wedding Bride WordPress theme before 1.0.2, Wlow WordPress theme before 1.2.7 suffer from the same issue about the search box reflecting the results causing XSS which allows an unauthenticated attacker to exploit against users if they click a malicious link.	6.1	More Details
CVE-2023-41537	phpjabbers Business Directory Script 3.2 is vulnerable to Cross Site Scripting (XSS) via the keyword parameter.	6.1	More Details
CVE-2023-39510	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The`reports_admin.php` script displays reporting information about graphs, devices, data sources etc. CENSUS found that an adversary that is able to configure a malicious Device name, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/reports_admin.php` when the a graph with the maliciously altered device name is linked to the report. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	6.1	More Details
CVE-2023-37828	A cross-site scripting (XSS) vulnerability in General Solutions Steiner GmbH CASE 3 Taskmanagement V 3.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Tasktyp parameter.	6.1	More Details
CVE-2023-39710	Multiple cross-site scripting (XSS) vulnerabilities in Free and Open Source Inventory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name, Address, and Company parameters under the Add Customer section.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39703	A cross site scripting (XSS) vulnerability in the Markdown Editor component of Typora v1.6.7 allows attackers to execute arbitrary code via uploading a crafted Markdown file.	6.1	More Details
CVE-2023-40969	Senayan Library Management Systems SLIMS 9 Bulian v9.6.1 is vulnerable to Server Side Request Forgery (SSRF) via admin/modules/bibliography/pop_p2p.php.	6.1	More Details
CVE-2023-39512	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `data_sources.php` displays the data source management information (e.g. data source path, polling configuration, device name related to the datasource etc.) for different data visualizations of the _cacti_ app. _CENSUS_ found that an adversary that is able to configure a malicious device name, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/data_sources.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	6.1	More Details
CVE-2023-37830	A cross-site scripting (XSS) vulnerability in General Solutions Steiner GmbH CASE 3 Taskmanagement V 3.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter.	6.1	More Details
CVE-2023-37829	A cross-site scripting (XSS) vulnerability in General Solutions Steiner GmbH CASE 3 Taskmanagement V 3.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the notification.message parameter.	6.1	More Details
CVE-2023-41163	A Reflected Cross-site scripting (XSS) vulnerability in the file manager tab in Usermin 2.000 allows remote attackers to inject arbitrary web script or HTML via the replace in results field while replacing the results under the tools drop down.	6.1	More Details
CVE-2023-37826	A cross-site scripting (XSS) vulnerability in General Solutions Steiner GmbH CASE 3 Taskmanagement V 3.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the fieldname parameter.	6.1	More Details
CVE-2023-37827	A cross-site scripting (XSS) vulnerability in General Solutions Steiner GmbH CASE 3 Taskmanagement V 3.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the executionBlockName parameter.	6.1	More Details
CVE-2023-25465	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy wp tell a friend popup form plugin <= 7.1 versions.	5.9	More Details
CVE-2023-36382	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jeffrey-WP Media Library Categories plugin <= 2.0.0 versions.	5.9	More Details
CVE-2023-22870	IBM Aspera Faspex 5.0.5 transmits sensitive information in cleartext which could be obtained by an attacker using man in the middle techniques. IBM X-Force ID: 244121.	5.9	More Details
CVE-2023-39919	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in maennchen1.De wpShopGermany – Protected Shops plugin <= 2.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39987	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ajay Lulia wSecure Lite plugin <= 2.5 versions.	5.9	More Details
CVE-2023-40206	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in hwk-fr WP 404 Auto Redirect to Similar Post plugin <= 1.0.3 versions.	5.9	More Details
CVE-2023-38518	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Visualmodo Borderless plugin <= 1.4.8 versions.	5.9	More Details
CVE-2023-31171	An Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in the Schweitzer Engineering Laboratories SEL-5030 acSELerator QuickSet Software could allow an attacker to embed instructions that could be executed by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5030 acSELerator QuickSet Software: through 7.1.3.0.	5.9	More Details
CVE-2023-32294	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Radical Web Design GDPR Cookie Consent Notice Box plugin <= 1.1.6 versions.	5.9	More Details
CVE-2023-37986	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in miniOrange YourMembership Single Sign On – YM SSO Login plugin <= 1.1.3 versions.	5.9	More Details
CVE-2023-41180	Incorrect certificate validation in InvokeHTTP on Apache NiFi MiNiFi C++ versions 0.13 to 0.14 allows an intermediary to present a forged certificate during TLS handshake negotation. The Disable Peer Verification property of InvokeHTTP was effectively flipped, disabling verification by default, when using HTTPS. Mitigation: Set the Disable Peer Verification property of InvokeHTTP to true when using MiNiFi C++ versions 0.13.0 or 0.14.0. Upgrading to MiNiFi C++ 0.15.0 corrects the default behavior.	5.9	More Details
CVE-2023-38521	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Exifography plugin <= 1.3.1 versions.	5.9	More Details
CVE-2023-31170	An Inclusion of Functionality from Untrusted Control Sphere vulnerability in the Schweitzer Engineering Laboratories SEL-5030 acSELerator QuickSet Software could allow an attacker to embed instructions that could be executed by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5030 acSELerator QuickSet Software: through 7.1.3.0.	5.9	More Details
CVE-2023-25488	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Duc Bui Quang WP Default Feature Image plugin <= 1.0.1.1 versions.	5.9	More Details
CVE-2023-25477	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Yotuwp Video Gallery plugin <= 1.3.12 versions.	5.9	More Details
CVE-2023-31172	An Incomplete Filtering of Special Elements vulnerability in the Schweitzer Engineering Laboratories SEL-5030 acSELerator QuickSet Software could allow an attacker to embed instructions that could be executed by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5030 acSELerator QuickSet Software: through 7.1.3.0.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38517	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Realwebcare WRC Pricing Tables plugin <= 2.3.7 versions.	5.9	More Details
CVE-2023-38482	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in QualityUnit Post Affiliate Pro plugin <= 1.25.0 versions.	5.9	More Details
CVE-2023-38476	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SuiteDash :: ONE Dashboard® Client Portal : SuiteDash Direct Login plugin <= 1.7.6 versions.	5.9	More Details
CVE-2023-25044	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sumo Social Share Boost plugin <= 4.4 versions.	5.9	More Details
CVE-2023-25042	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Liam Gladdy (Storm Consultancy) oAuth Twitter Feed for Developers plugin <= 2.3.0 versions.	5.9	More Details
CVE-2023-24412	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Web-Settler Image Social Feed plugin <= 1.7.6 versions.	5.9	More Details
CVE-2023-38387	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Elastic Email Sender plugin <= 1.2.6 versions.	5.9	More Details
CVE-2023-39354	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Read in the `nsc_rle_decompress_data` function. The Out-Of-Bounds Read occurs because it processes `context->Planes` without checking if it contains data of sufficient length. Should an attacker be able to leverage this vulnerability they may be able to cause a crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.9	More Details
CVE-2023-34372	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Didier Sampaolo SpamReferrerBlock plugin <= 2.22 versions.	5.9	More Details
CVE-2023-35092	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Abhay Yadav Breadcrumb simple plugin <= 1.3 versions.	5.9	More Details
CVE-2023-28692	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kevon Adonis WP Abstracts plugin <= 2.6.3 versions.	5.9	More Details
CVE-2023-34173	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alexander Semikashev Yandex Metrica Counter plugin <= 1.4.3 versions.	5.9	More Details
CVE-2023-32962	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in HasTheme WishSuite – Wishlist for WooCommerce plugin <= 1.3.4 versions.	5.9	More Details
CVE-2023-25462	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP htaccess Control plugin <= 3.5.1 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27426	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Notifyvisitors NotifyVisitors plugin <= 1.0 versions.	5.9	More Details
CVE-2023-33208	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gsmith Cookie Monster plugin <= 1.51 versions.	5.9	More Details
CVE-2023-33210	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in nuajik plugin <= 0.1.0 versions.	5.9	More Details
CVE-2023-33929	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joaquín Ruiz Easy Admin Menu plugin <= 1.3 versions.	5.9	More Details
CVE-2023-34183	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Valiano Unite Gallery Lite plugin <= 1.7.61 versions.	5.9	More Details
CVE-2023-28415	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in XootiX Side Cart Woocommerce (Ajax) plugin <= 2.2 versions.	5.9	More Details
CVE-2023-34172	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Miled WordPress Social Login plugin <= 3.0.4 versions.	5.9	More Details
CVE-2023-34187	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alan Tien Call Now Icon Animate plugin <= 0.1.0 versions.	5.9	More Details
CVE-2023-24397	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Reservation.Studio Reservation.Studio widget plugin <= 1.0.11 versions.	5.9	More Details
CVE-2023-24401	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Davidsword Mobile Call Now & Map Buttons plugin <= 1.5.0 versions.	5.9	More Details
CVE-2023-27621	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in MrDemonWolf Livestream Notice plugin <= 1.2.0 versions.	5.9	More Details
CVE-2023-39350	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. This issue affects Clients only. Integer underflow leading to DOS (e.g. abort due to `WINPR_ASSERT` with default compilation flags). When an insufficient blockLen is provided, and proper length validation is not performed, an Integer Underflow occurs, leading to a Denial of Service (DOS) vulnerability. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.9	More Details
CVE-2023-32740	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Kunal Nagar Custom 404 Pro plugin <= 3.8.1 versions.	5.8	More Details
CVE-2023-31423	Possible information exposure through log file vulnerability where sensitive fields are recorded in the configuration log without masking on Brocade SANnav before v2.3.0 and 2.2.2a. Notes: To access the logs, the local attacker must have access to an already collected Brocade SANnav "supportsave" outputs.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3950	An information disclosure issue in GitLab EE affecting all versions from 16.2 prior to 16.2.5, and 16.3 prior to 16.3.1 allowed other Group Owners to see the Public Key for a Google Cloud Logging audit event streaming destination, if configured. Owners can now only write the key, not read it.	5.5	More Details
CVE-2023-4378	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.8 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. A malicious Maintainer can, under specific circumstances, leak the sentry token by changing the configured URL in the Sentry error tracking settings page. This was as a result of an incomplete fix for CVE-2022-4365.	5.5	More Details
CVE-2023-4756	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-4754	Out-of-bounds Write in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-38439	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-4688	Sensitive information leak through log files. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 35433.	5.5	More Details
CVE-2023-41751	Sensitive information disclosure due to improper token expiration validation. The following products are affected: Acronis Agent (Windows) before build 32047.	5.5	More Details
CVE-2023-41750	Sensitive information disclosure due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 32047.	5.5	More Details
CVE-2023-38438	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-4683	NULL Pointer Dereference in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-4755	Use After Free in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-4682	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-4758	Buffer Over-read in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-4681	NULL Pointer Dereference in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4678	Divide By Zero in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-41057	hyper-bump-it is a command line tool for updating the version in project files.`hyper-bump-it` reads a file glob pattern from the configuration file. That is combined with the project root directory to construct a full glob pattern that is used to find files that should be edited. These matched files should be contained within the project root directory, but that is not checked. This could result in changes being written to files outside of the project. The default behaviour of `hyper-bump-it` is to display the planned changes and prompt the user for confirmation before editing any files. However, the configuration file provides a field that can be used cause files to be edited without displaying the prompt. This issue has been fixed in release version 0.5.1. Users are advised to upgrade. Users that are unable to update from vulnerable versions, executing `hyper-bump-it` with the `--interactive` command line argument will ensure that all planned changes are displayed and prompt the user for confirmation before editing any files, even if the configuration file contains `show_confirm_prompt=true`.	5.5	More Details
CVE-2023-41717	Inappropriate file type control in Zscaler Proxy versions 3.6.1.25 and prior allows local attackers to bypass file download/upload restrictions.	5.5	More Details
CVE-2023-4721	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-36308	disintegration Imaging 1.6.2 allows attackers to cause a panic (because of an integer index out of range during a Grayscale call) via a crafted TIFF file to the scan function of scanner.go. NOTE: it is unclear whether there are common use cases in which this panic could have any security consequence	5.5	More Details
CVE-2023-36307	ZPLGFA 1.1.1 allows attackers to cause a panic (because of an integer index out of range during a ConvertToGraphicField call) via an image of zero width. NOTE: it is unclear whether there are common use cases in which this panic could have any security consequence	5.5	More Details
CVE-2023-31168	An Inclusion of Functionality from Untrusted Control Sphere vulnerability in the Schweitzer Engineering Laboratories SEL-5030 acSELerator QuickSet Software could allow an attacker to embed instructions that could be executed by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5030 acSELerator QuickSet Software: through 7.1.3.0.	5.5	More Details
CVE-2023-39136	An unhandled edge case in the component _sanitizedPath of ZipArchive v2.5.4 allows attackers to cause a Denial of Service (DoS) via a crafted zip file.	5.5	More Details
CVE-2023-4480	Due to an out-of-date dependency in the “Fusion File Manager” component accessible through the admin panel, an attacker can send a crafted request that allows them to read the contents of files on the system accessible within the privileges of the running process. Additionally, they may write files to arbitrary locations, provided the files pass the application’s mime-type and file extension validation.	5.5	More Details
CVE-2023-4778	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-4720	Floating Point Comparison with Incorrect Operator in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41745	Sensitive information disclosure due to excessive collection of system information. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 30991, Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 35979.	5.5	More Details
CVE-2023-4722	Integer Overflow or Wraparound in GitHub repository gpac/gpac prior to 2.3-DEV.	5.5	More Details
CVE-2023-20825	In duraspeed, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07951402; Issue ID: ALPS07951413.	5.5	More Details
CVE-2023-38446	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-38447	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-41633	Catdoc v0.95 was discovered to contain a NULL pointer dereference via the component xls2csv at src/fileutil.c.	5.5	More Details
CVE-2023-38448	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-33918	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-33917	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-4712	A vulnerability, which was classified as critical, was found in Xintian Smart Table Integrated Management System 5.6.9. This affects an unknown part of the file /SysManage/AddUpdateRole.aspx. The manipulation of the argument txtRoleName leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-238575. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-20826	In cta, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07978550; Issue ID: ALPS07978550.	5.5	More Details
CVE-2023-20824	In duraspeed, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07951402; Issue ID: ALPS07951402.	5.5	More Details
CVE-2023-38436	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38554	In wcn bsp driver, there is a possible out of bounds write due to a missing bounds check.This could lead to local denial of service with no additional execution privileges	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33916	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38466	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38465	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38454	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38457	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-38461	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-38463	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-38445	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-4713	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. This vulnerability affects the function addComment of the file ?r=weibo/comment/addcomment. The manipulation of the argument touid leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-238576. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-38462	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-38442	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38437	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38441	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-38440	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31925	Brocade SANnav before v2.3.0 and v2.2.2a stores SNMPv3 Authentication passwords in plaintext. A privileged user could retrieve these credentials with knowledge and access to these log files. SNMP credentials could be seen in SANnav SupportSave if the capture is performed after an SNMP configuration failure causes an SNMP communication log dump.	5.4	More Details
CVE-2023-4649	Session Fixation in GitHub repository instantsoft/icms2 prior to 2.16.1.	5.4	More Details
CVE-2023-4651	Server-Side Request Forgery (SSRF) in GitHub repository instantsoft/icms2 prior to 2.16.1.	5.4	More Details
CVE-2023-4652	Cross-site Scripting (XSS) - Stored in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	5.4	More Details
CVE-2023-38970	Cross Site Scripting vulnerabiltiy in Badaso v.0.0.1 thru v.2.9.7 allows a remote attacker to execute arbitrary code via a crafted payload to the Name of member parameter in the add new member function.	5.4	More Details
CVE-2023-2171	The BadgeOS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in versions up to, and including, 3.7.1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2023-2279	The WP Directory Kit plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.1. This is due to missing or incorrect nonce validation on the 'admin_page_display' function. This makes it possible for unauthenticated attackers to delete or change plugin settings, import demo data, modify or delete Directory Kit related posts and terms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Partial patches were made avilable in versions 1.2.0 and 1.2.1 but the issue was not fully patched until 1.2.2	5.4	More Details
CVE-2023-41107	TEF portal 2023-07-17 is vulnerable to a persistent cross site scripting (XSS)attack.	5.4	More Details
CVE-2022-22305	An improper certificate validation vulnerability [CWE-295] in FortiManager 7.0.1 and below, 6.4.6 and below; FortiAnalyzer 7.0.2 and below, 6.4.7 and below; FortiOS 6.2.x and 6.0.x; FortiSandbox 4.0.x, 3.2.x and 3.1.x may allow a network adjacent and unauthenticated attacker to man-in-the-middle the communication between the listed products and some external peers.	5.4	More Details
CVE-2023-40705	Stored cross-site scripting vulnerability in Map setting page of VI Web Client prior to 7.9.6 allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-4035	The Simple Blog Card WordPress plugin before 1.31 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-2023-40535	Stored cross-site scripting vulnerability in View setting page of VI Web Client prior to 7.9.6 allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2020-10128	SearchBlox product with version before 9.2.1 is vulnerable to stored cross-site scripting at multiple user input parameters. In SearchBlox products multiple parameters are not sanitized/validate properly which allows an attacker to inject malicious JavaScript.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38569	Stored cross-site scripting vulnerability in SHIRASAGI prior to v1.18.0 allows a remote authenticated attacker to execute an arbitrary script on the web browser of the user who is logging in to the product.	5.4	More Details
CVE-2023-34637	A stored cross-site scripting (XSS) vulnerability in IsarNet AG IsarFlow v5.23 allows authenticated attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the dashboard title parameter in the IsarFlow Portal.	5.4	More Details
CVE-2022-44349	NAVBLUE S.A.S N-Ops & Crew 22.5-rc.50 is vulnerable to Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-39356	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. In affected versions a missing offset validation may lead to an Out Of Bound Read in the function `gdi_multi_opaque_rect`. In particular there is no code to validate if the value `multi_opaque_rect->numRectangles` is less than 45. Looping through `multi_opaque_rect->`numRectangles without proper boundary checks can lead to Out-of-Bounds Read errors which will likely lead to a crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-39983	A vulnerability that poses a potential risk of polluting the MXsecurity sqlite database and the nsm-web UI has been identified in MXsecurity versions prior to v1.0.1. This vulnerability might allow an unauthenticated remote attacker to register or add devices via the nsm-web application.	5.3	More Details
CVE-2023-4647	An issue has been discovered in GitLab affecting all versions starting from 15.2 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1 in which the projects API pagination can be skipped, potentially leading to DoS on certain instances.	5.3	More Details
CVE-2023-35906	IBM Aspera Faspex 5.0.5 could allow a remote attacked to bypass IP restrictions due to improper access controls. IBM X-Force ID: 259649.	5.3	More Details
CVE-2023-40188	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Read in the `general_LumaToYUV444` function. This Out-Of-Bounds Read occurs because processing is done on the `in` variable without checking if it contains data of sufficient length. Insufficient data for the `in` variable may cause errors or crashes. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2023-39353	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to a missing offset validation leading to Out Of Bound Read. In the `libfreerdp/codec/rfx.c` file there is no offset validation in `tile->quantIdxY`, `tile->quantIdxCb`, and `tile->quantIdxCr`. As a result crafted input can lead to an out of bounds read access which in turn will cause a crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-3221	User enumeration vulnerability in Password Recovery plugin 1.2 version for Roundcube, which could allow a remote attacker to create a test script against the password recovery function to enumerate all users in the database.	5.3	More Details
CVE-2023-41741	Exposure of sensitive information to an unauthorized actor vulnerability in cgi component in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote attackers to obtain sensitive information via unspecified vectors.	5.3	More Details
CVE-2023-41740	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in cgi component in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote attackers to read specific files via unspecified vectors.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40575	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Read in the `general_YUV444ToRGB_8u_P3AC4R_BGRX` function. This issue is likely down to insufficient data for the `pSrc` variable and results in crashes. This issue has been addressed in version 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2023-40576	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Out-Of-Bounds Read in the `RleDecompress` function. This Out-Of-Bounds Read occurs because FreeRDP processes the `pbSrcBuffer` variable without checking if it contains data of sufficient length. Insufficient data in the `pbSrcBuffer` variable may cause errors or crashes. This issue has been addressed in version 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2023-20897	Salt masters prior to 3005.2 or 3006.2 contain a DOS in minion return. After receiving several bad packets on the request server equal to the number of worker threads, the master will become unresponsive to return requests until restarted.	5.3	More Details
CVE-2023-41908	Cerebrate before 1.15 lacks the Secure attribute for the session cookie.	5.3	More Details
CVE-2023-39351	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions of FreeRDP are subject to a Null Pointer Dereference leading a crash in the RemoteFX (rfx) handling. Inside the `rfx_process_message_tileset` function, the program allocates tiles using `rfx_allocate_tiles` for the number of numTiles. If the initialization process of tiles is not completed for various reasons, tiles will have a NULL pointer. Which may be accessed in further processing and would cause a program crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-23763	An authorization/sensitive information disclosure vulnerability was identified in GitHub Enterprise Server that allowed a fork to retain read access to an upstream repository after its visibility was changed to private. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.10.0 and was fixed in versions 3.9.4, 3.8.9, 3.7.16 and 3.6.18. This vulnerability was reported via the GitHub Bug Bounty program.	5.3	More Details
CVE-2022-1601	The User Access Manager WordPress plugin before 2.2.18 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible for attackers to access restricted content in certain situations.	5.3	More Details
CVE-2023-39352	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an invalid offset validation leading to Out Of Bound Write. This can be triggered when the values `rect->left` and `rect->top` are exactly equal to `surface->width` and `surface->height`. eg. `rect->left` == `surface->width` && `rect->top` == `surface->height`. In practice this should cause a crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-40181	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. Affected versions are subject to an Integer-Underflow leading to Out-Of-Bound Read in the `zgfx_decompress_segment` function. In the context of `CopyMemory`, it's possible to read data beyond the transmitted packet range and likely cause a crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-33220	Information disclosure in Automotive multimedia due to buffer over-read.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29261	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 could allow a local user with specific information about the system to obtain privileged information due to inadequate memory clearing during operations. IBM X-Force ID: 252139.	5.1	More Details
CVE-2023-32338	IBM Sterling Secure Proxy and IBM Sterling External Authentication Server 6.0.3 and 6.1.0 stores user credentials in plain clear text which can be read by a local user with container access. IBM X-Force ID: 255585.	5.1	More Details
CVE-2022-4343	An issue has been discovered in GitLab EE affecting all versions starting from 13.12 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1 in which a project member can leak credentials stored in site profile.	5.0	More Details
CVE-2023-31167	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Schweitzer Engineering Laboratories SEL-5036 acSELerator Bay Screen Builder Software on Windows allows Relative Path Traversal. SEL acSELerator Bay Screen Builder software is distributed by SEL-5033 SEL acSELerator RTAC, SEL-5030 Quickset, and SEL Compass. CVE-2023-31167 and was patched in the acSELerator Bay Screen Builder release available on 20230602. Please contact SEL for additional details. This issue affects SEL-5036 acSELerator Bay Screen Builder Software: before 1.0.49152.778.	5.0	More Details
CVE-2023-4711	A vulnerability, which was classified as critical, has been found in D-Link DAR-8000-10 up to 20230819. Affected by this issue is some unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to os command injection. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. VDB-238574 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2023-39912	Zoho ManageEngine ADManager Plus before 7203 allows Help Desk Technician users to read arbitrary files on the machine where this product is installed.	4.9	More Details
CVE-2022-3407	I some cases, when the device is USB-tethered to a host PC, and the device is sharing its mobile network connection with the host PC, if the user originates a call on the device, then the device's modem may reset and cause the phone call to not succeed. This may block the user from dialing emergency services. This patch resolves the device's modem reset issue.	4.9	More Details
CVE-2023-3404	The ProfileGrid plugin for WordPress is vulnerable to unauthorized decryption of private information in versions up to, and including, 5.5.0. This is due to the passphrase and iv being hardcoded in the 'pm_encrypt_decrypt_pass' function and used across all sites running the plugin. This makes it possible for authenticated attackers, with administrator-level permissions or above to decrypt and view users' passwords. If combined with another vulnerability, this can potentially grant lower-privileged users access to users' passwords.	4.9	More Details
CVE-2023-39582	SQL Injection vulnerability in Chamilo LMS v.1.11 thru v.1.11.20 allows a remote privileged attacker to obtain sensitive information via the import sessions functions.	4.9	More Details
CVE-2023-2354	The CHP Ads Block Detector plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings reachable though an AJAX action in versions up to, and including, 3.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.9	More Details
CVE-2023-3814	The Advanced File Manager WordPress plugin before 5.1.1 does not adequately authorize its usage on multisite installations, allowing site admin users to list and read arbitrary files and folders on the server.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4704	External Control of System or Configuration Setting in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	4.9	More Details
CVE-2023-41739	Uncontrolled resource consumption vulnerability in File Functionality in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote authenticated users to conduct denial-of-service attacks via unspecified vectors.	4.9	More Details
CVE-2021-40546	Tenda AC6 US_AC6V4.0RTL_V02.03.01.26_cn.bin allows attackers (who have the administrator password) to cause a denial of service (device crash) via a long string in the wifiPwd_5G parameter to /goform/setWifi.	4.9	More Details
CVE-2023-4253	The AI ChatBot WordPress plugin before 4.7.8 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-2023-37222	Farsight Tech Nordic AB ProVide version 14.5 - Multiple XSS vulnerabilities (CWE-79) can be exploited by a user with administrator privilege.	4.8	More Details
CVE-2023-31169	An Improper Handling of Unicode Encoding vulnerability in the Schweitzer Engineering Laboratories SEL-5030 acSELerator QuickSet Software could allow an attacker to embed instructions that could be executed by an authorized device operator. See Instruction Manual Appendix A and Appendix E dated 20230615 for more details. This issue affects SEL-5030 acSELerator QuickSet Software: through 7.1.3.0.	4.8	More Details
CVE-2023-3499	The Photo Gallery, Images, Slider in Rbs Image Gallery WordPress plugin before 3.2.16 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-2023-4298	The 123.chat WordPress plugin before 1.3.1 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-2023-4254	The AI ChatBot WordPress plugin before 4.7.8 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-2023-3501	The FormCraft WordPress plugin before 1.2.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-4653	Cross-site Scripting (XSS) - Stored in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	4.8	More Details
CVE-2023-24675	Cross Site Scripting Vulnerability in BluditCMS v.3.14.1 allows attackers to execute arbitrary code via the Categories Friendly URL.	4.8	More Details
CVE-2023-4109	The Ninja Forms WordPress Ninja Forms Contact Form WordPress plugin before 3.6.26 was affected by a HTML Injection security vulnerability.	4.8	More Details
CVE-2023-1982	The Front Editor WordPress plugin through 4.0.4 does not sanitize and escape some of its form settings, which could allow high-privilege users 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 Number	Description	Base Score	Reference
CVE-2023-23765	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff in a re-opened Pull Request. To exploit this vulnerability, an attacker would need write access to the repository. This vulnerability was reported via the GitHub Bug Bounty Program https://bounty.github.com/ .	4.8	More Details
CVE-2023-36811	borgbackup is an opensource, deduplicating archiver with compression and authenticated encryption. A flaw in the cryptographic authentication scheme in borgbackup allowed an attacker to fake archives and potentially indirectly cause backup data loss in the repository. The attack requires an attacker to be able to: 1. insert files (with no additional headers) into backups and 2. gain write access to the repository. This vulnerability does not disclose plaintext to the attacker, nor does it affect the authenticity of existing archives. Creating plausible fake archives may be feasible for empty or small archives, but is unlikely for large archives. The issue has been fixed in borgbackup 1.2.5. Users are advised to upgrade. Additionally to installing the fixed code, users must follow the upgrade procedure as documented in the change log. Data loss after being attacked can be avoided by reviewing the archives (timestamp and contents valid and as expected) after any "borg check --repair" and before "borg prune". There are no known workarounds for this vulnerability.	4.7	More Details
CVE-2023-4650	Improper Access Control in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	4.7	More Details
CVE-2023-4500	The Order Tracking Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the order status parameter in versions up to, and including, 3.3.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers (admin or higher) to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.7	More Details
CVE-2023-39365	Cacti is an open source operational monitoring and fault management framework. Issues with Cacti Regular Expression validation combined with the external links feature can lead to limited SQL Injections and subsequent data leakage. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.6	More Details
CVE-2023-32817	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08044040; Issue ID: ALPS08044035.	4.4	More Details
CVE-2023-38467	In urild service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-32815	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08037801; Issue ID: ALPS08037801.	4.4	More Details
CVE-2023-32814	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08031947; Issue ID: ALPS08031947.	4.4	More Details
CVE-2023-32813	In gnss service, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017370; Issue ID: ALPS08017370.	4.4	More Details
CVE-2023-20823	In cmdq, there is a possible out of bounds read due to an incorrect status check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08021592; Issue ID: ALPS08021592.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4162	A segmentation fault can occur in Brocade Fabric OS after Brocade Fabric OS v9.0 and before Brocade Fabric OS v9.2.0a through the passwdcfg command. This could allow an authenticated privileged user local user to crash a Brocade Fabric OS swith using the cli “passwdcfg --set -expire -minDiff“.	4.4	More Details
CVE-2023-4163	In Brocade Fabric OS before v9.2.0a, a local authenticated privileged user can trigger a buffer overflow condition, leading to a kernel panic with large input to buffers in the portcfgfportbuffers command.	4.4	More Details
CVE-2023-20836	In camsys, 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: ALPS07505629; Issue ID: ALPS07505629.	4.4	More Details
CVE-2023-32816	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08044040; Issue ID: ALPS08044032.	4.4	More Details
CVE-2023-38468	In urild service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2022-48453	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-4636	The WordPress File Sharing Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 2.0.3 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-2022-48452	In Ifaa service, there is a possible missing permission check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-32808	In bluetooth driver, there is a possible read and write access to registers due to improper access control of register interface. This could lead to local leak of sensitive information with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07849751; Issue ID: ALPS07849751.	4.4	More Details
CVE-2022-47353	In vdsp device, there is a possible system crash due to improper input validation.This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2022-47352	In camera driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-4160	The WooCommerce PDF Invoice Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 1.2.90 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 Number	Description	Base Score	Reference
CVE-2023-32807	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588360; Issue ID: ALPS07588360.	4.4	More Details
CVE-2023-32810	In bluetooth driver, there is a possible out of bounds read due to improper input validation. This could lead to local information leak with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07867212; Issue ID: ALPS07867212.	4.4	More Details
CVE-2023-32809	In bluetooth driver, there is a possible read and write access to registers due to improper access control of register interface. This could lead to local leak of sensitive information with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07849753; Issue ID: ALPS07849753.	4.4	More Details
CVE-2023-20833	In keyinstall, there is a possible information disclosure 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: ALPS08017756; Issue ID: ALPS08017764.	4.4	More Details
CVE-2023-4150	The User Activity Tracking and Log WordPress plugin before 4.0.9 does not have proper CSRF checks when managing its license, which could allow attackers to make logged in admins update and deactivate the plugin's license via CSRF attacks	4.3	More Details
CVE-2023-3356	The Subscribers Text Counter WordPress plugin before 1.7.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack, which also lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping	4.3	More Details
CVE-2023-4023	The All Users Messenger WordPress plugin through 1.24 does not prevent non-administrator users from deleting messages from the all-users messenger.	4.3	More Details
CVE-2023-4600	The AffiliateWP for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'affwp_activate_addons_page_plugin' function called via an AJAX action in versions up to, and including, 2.14.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to activate arbitrary plugins.	4.3	More Details
CVE-2023-4209	The POEditor WordPress plugin before 0.9.8 does not have CSRF checks in various places, which could allow attackers to make logged in admins perform unwanted actions, such as reset the plugin's settings and update its API key via CSRF attacks.	4.3	More Details
CVE-2023-4036	The Simple Blog Card WordPress plugin before 1.32 does not ensure that posts to be displayed via a shortcode are public, allowing any authenticated users, such as subscriber, to retrieve arbitrary post title and their content such as draft, private and password protected ones	4.3	More Details
CVE-2023-30534	Cacti is an open source operational monitoring and fault management framework. There are two instances of insecure deserialization in Cacti version 1.2.24. While a viable gadget chain exists in Cacti’s vendor directory (phpseclib), the necessary gadgets are not included, making them inaccessible and the insecure deserializations not exploitable. Each instance of insecure deserialization is due to using the unserialize function without sanitizing the user input. Cacti has a “safe” deserialization that attempts to sanitize the content and check for specific values before calling unserialize, but it isn’t used in these instances. The vulnerable code lies in graphs_new.php, specifically within the host_new_graphs_save function. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2023-4522	An issue has been discovered in GitLab affecting all versions before 16.2.0. Committing directories containing LF character results in 500 errors when viewing the commit.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33834	IBM Security Verify Information Queue 10.0.4 and 10.0.5 could allow a remote attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-force ID: 256014.	4.3	More Details
CVE-2023-33835	IBM Security Verify Information Queue 10.0.4 and 10.0.5 could allow a remote attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 256015.	4.3	More Details
CVE-2023-3764	The WooCommerce PDF Invoice Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.90. This is due to missing or incorrect nonce validation on the Save function. This makes it possible for unauthenticated attackers to make changes to invoices 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-2023-4269	The User Activity Log WordPress plugin before 1.6.6 lacks proper authorisation when exporting its activity logs, allowing any authenticated users, such as subscriber to perform such action and retrieve PII such as email addresses.	4.3	More Details
CVE-2023-40589	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. In affected versions there is a Global-Buffer-Overflow in the ncrush_decompress function. Feeding crafted input into this function can trigger the overflow which has only been shown to cause a crash. This issue has been addressed in versions 2.11.0 and 3.0.0-beta3. Users are advised to upgrade. There are no known workarounds for this issue.	4.3	More Details
CVE-2023-4709	A vulnerability classified as problematic has been found in TOTVS RM 12.1. Affected is an unknown function of the file Login.aspx of the component Portal. The manipulation of the argument VIEWSTATE leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-238572. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4714	A vulnerability was found in PlayTube 3.0.1 and classified as problematic. This issue affects some unknown processing of the component Redirect Handler. The manipulation leads to information disclosure. The attack may be initiated remotely. The identifier VDB-238577 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2022-43903	IBM Security Guardium 10.6, 11.3, and 11.4 could allow an authenticated user to cause a denial of service due to due to improper input validation. IBM X-Force ID: 240894.	4.3	More Details
CVE-2023-4018	An issue has been discovered in GitLab affecting all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. Due to improper permission validation it was possible to create model experiments in public projects.	4.3	More Details
CVE-2023-4059	The Profile Builder WordPress plugin before 3.9.8 lacks authorisation and CSRF in its page creation function which allows unauthenticated users to create the register, log-in and edit-profile pages from the plugin on the blog	4.3	More Details
CVE-2023-4245	The WooCommerce PDF Invoice Builder for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the GetInvoiceDetail function in versions up to, and including, 1.2.89. This makes it possible for subscribers to view arbitrary invoices provided they can guess the order id and invoice id.	4.3	More Details
CVE-2023-4161	The WooCommerce PDF Invoice Builder for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the SaveCustomField function in versions up to, and including, 1.2.90. This makes it possible for unauthenticated attackers to create invoice fields provided they can trick an admin into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4710	A vulnerability classified as problematic was found in TOTVS RM 12.1. Affected by this vulnerability is an unknown functionality of the component Portal. The manipulation of the argument d leads to cross site scripting. The attack can be launched remotely. The identifier VDB-238573 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-2172	The BadgeOS plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.7.1.6. This is due to improper validation and authorization checks within the badgeos_update_steps_ajax_handler, badgeos_update_award_steps_ajax_handler, badgeos_update_deduct_steps_ajax_handler, and badgeos_update_ranks_req_steps_ajax_handler functions. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to overwrite arbitrary post titles.	4.3	More Details
CVE-2023-2352	The CHP Ads Block Detector plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.9.4. This is due to missing or incorrect nonce validation on the chp_abd_action function. This makes it possible for unauthenticated attackers to update or reset plugin 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-2023-0689	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Information Disclosure via the 'mf_first_name' shortcode in versions up to, and including, 3.3.1. This allows authenticated attackers, with subscriber-level capabilities or above to obtain sensitive information about arbitrary form submissions, including the submitter's first name.	4.3	More Details
CVE-2023-2174	The BadgeOS plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_badgeos_log_entries function in versions up to, and including, 3.7.1.6. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete the plugin's log entries.	4.3	More Details
CVE-2023-2353	The CHP Ads Block Detector plugin for WordPress is vulnerable to unauthorized plugin settings update and reset due to a missing capability check on the chp_abd_action function in versions up to, and including, 3.9.4. This makes it possible for subscriber-level attackers to change or reset plugin settings. CVE-2023-36509 appears to be a duplicate of this issue.	4.3	More Details
CVE-2023-20839	In imgsys, there is a possible out of bounds read due to a missing valid range checking. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326409.	4.2	More Details
CVE-2023-20898	Git Providers can read from the wrong environment because they get the same cache directory base name in Salt masters prior to 3005.2 or 3006.2. Anything that uses Git Providers with different environments can get garbage data or the wrong data, which can lead to wrongful data disclosure, wrongful executions, data corruption and/or crash.	4.2	More Details
CVE-2023-20847	In imgsys_cmdq, there is a possible out of bounds read due to a missing valid range checking. This could lead to local denial of service with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07354025; Issue ID: ALPS07340108.	4.2	More Details
CVE-2023-20845	In imgsys, there is a possible out of bounds read due to a missing valid range checking. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07197795; Issue ID: ALPS07340357.	4.2	More Details
CVE-2023-20843	In imgsys_cmdq, there is a possible out of bounds read due to a missing valid range checking. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07340119; Issue ID: ALPS07340119.	4.2	More Details
CVE-2023-20846	In imgsys_cmdq, there is a possible out of bounds read due to a missing valid range checking. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07354023; Issue ID: ALPS07340098.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20844	In imgsys_cmdq, there is a possible out of bounds read due to a missing valid range checking. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07354058; Issue ID: ALPS07340121.	4.2	More Details
CVE-2023-20838	In imgsys, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326418.	4.0	More Details
CVE-2023-41040	GitPython is a python library used to interact with Git repositories. In order to resolve some git references, GitPython reads files from the `.git` directory, in some places the name of the file being read is provided by the user, GitPython doesn't check if this file is located outside the `.git` directory. This allows an attacker to make GitPython read any file from the system. This vulnerability is present in https://github.com/gitpython-developers/GitPython/blob/1c8310d7cae144f74a671cbe17e51f63a830adbf/git/refs/symbolic.py#L174-L175. That code joins the base directory with a user given string without checking if the final path is located outside the base directory. This vulnerability cannot be used to read the contents of files but could in theory be used to trigger a denial of service for the program. This issue has been addressed in version 3.1.37.	4.0	More Details
CVE-2023-41052	Vyper is a Pythonic Smart Contract Language. In affected versions the order of evaluation of the arguments of the builtin functions `uint256_addmod`, `uint256_mulmod`, `ecadd` and `ecmul` does not follow source order. This behaviour is problematic when the evaluation of one of the arguments produces side effects that other arguments depend on. A patch is currently being developed on pull request #3583. When using builtins from the list above, users should make sure that the arguments of the expression do not produce side effects or, if one does, that no other argument is dependent on those side effects.	3.7	More Details
CVE-2023-40015	Vyper is a Pythonic Smart Contract Language. For the following (probably non-exhaustive) list of expressions, the compiler evaluates the arguments from right to left instead of left to right. `unsafe_add, unsafe_sub, unsafe_mul, unsafe_div, pow_mod256, |, &, ^ (bitwise operators), bitwise_or (deprecated), bitwise_and (deprecated), bitwise_xor (deprecated), raw_call, <, >, <=, >=, ==, !=, in, not in (when lhs and rhs are enums)`. This behaviour becomes a problem when the evaluation of one of the arguments produces side effects that other arguments depend on. The following expressions can produce side-effect: state modifying external call , state modifying internal call, `raw_call`, `pop()` when used on a Dynamic Array stored in the storage, `create_minimal_proxy_to`, `create_copy_of`, `create_from_blueprint`. This issue has not yet been patched. Users are advised to make sure that the arguments of the expression do not produce side effects or, if one does, that no other argument is dependent on those side effects.	3.7	More Details
CVE-2023-41045	Graylog is a free and open log management platform. Graylog makes use of only one single source port for DNS queries. Graylog binds a single socket for outgoing DNS queries and while that socket is bound to a random port number it is never changed again. This goes against recommended practice since 2008, when Dan Kaminsky discovered how easy is to carry out DNS cache poisoning attacks. In order to prevent cache poisoning with spoofed DNS responses, it is necessary to maximise the uncertainty in the choice of a source port for a DNS query. Although unlikely in many setups, an external attacker could inject forged DNS responses into a Graylog's lookup table cache. In order to prevent this, it is at least recommendable to distribute the DNS queries through a pool of distinct sockets, each of them with a random source port and renew them periodically. This issue has been addressed in versions 5.0.9 and 5.1.3. Users are advised to upgrade. There are no known workarounds for this issue.	3.7	More Details
CVE-2023-4707	A vulnerability was found in Infosoftbd Clcknshop 1.0.0. It has been declared as problematic. This vulnerability affects unknown code of the file /collection/all. The manipulation of the argument q leads to cross site scripting. The attack can be initiated remotely. VDB-238570 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0120	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. Due to improper permission validation it was possible to edit labels description by an unauthorised user.	3.5	More Details
CVE-2023-39364	Cacti is an open source operational monitoring and fault management framework. In Cacti 1.2.24, users with console access can be redirected to an arbitrary website after a change password performed via a specifically crafted URL. The `auth_changepassword.php` file accepts `ref` as a URL parameter and reflects it in the form used to perform the change password. It's value is used to perform a redirect via `header` PHP function. A user can be tricked in performing the change password operation, e.g., via a phishing message, and then interacting with the malicious website where the redirection has been performed, e.g., downloading malwares, providing credentials, etc. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.5	More Details
CVE-2023-4654	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository instantsoft/icms2 prior to 2.16.1.	3.5	More Details
CVE-2023-41044	Graylog is a free and open log management platform. A partial path traversal vulnerability exists in Graylog's `Support Bundle` feature. The vulnerability is caused by incorrect user input validation in an HTTP API resource. Graylog's Support Bundle feature allows an attacker with valid Admin role credentials to download or delete files in sibling directories of the support bundle directory. The default `data_dir` in operating system packages (DEB, RPM) is set to `/var/lib/graylog-server`. The data directory for the Support Bundle feature is always `<data_dir>/support-bundle`. Due to the partial path traversal vulnerability, an attacker with valid Admin role credentials can read or delete files in directories that start with a `/var/lib/graylog-server/support-bundle` directory name. The vulnerability would allow the download or deletion of files in the following example directories: `/var/lib/graylog-server/support-bundle-test` and `/var/lib/graylog-server/support-bundlesdirectory`. For the Graylog Docker images, the `data_dir` is set to `/usr/share/graylog/data` by default. This vulnerability is fixed in Graylog version 5.1.3 and later. Users are advised to upgrade. Users unable to upgrade should block all HTTP requests to the following HTTP API endpoints by using a reverse proxy server in front of Graylog. `GET /api/system/debug/support/bundle/download/{filename}` and `DELETE /api/system/debug/support/bundle/{filename}`.	3.3	More Details
CVE-2023-35124	An information disclosure vulnerability exists in the OAS Engine configuration management functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted series of network requests can lead to a disclosure of sensitive information. An attacker can send a sequence of requests to trigger this vulnerability.	3.1	More Details
CVE-2023-4743	A vulnerability was found in Dreamer CMS up to 4.1.3. It has been classified as problematic. Affected is an unknown function of the file /upload/ueditorConfig?action=config. The manipulation leads to files or directories accessible. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-238632. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2023-34994	An improper resource allocation vulnerability exists in the OAS Engine configuration management functionality of Open Automation Software OAS Platform v18.00.0072. A specially crafted series of network requests can lead to creation of an arbitrary directory. An attacker can send a sequence of requests to trigger this vulnerability.	3.1	More Details
CVE-2023-33833	IBM Security Verify Information Queue 10.0.4 and 10.0.5 stores sensitive information in plain clear text which can be read by a local user. IBM X-Force ID: 256013.	2.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1555	An issue has been discovered in GitLab affecting all versions starting from 15.2 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1. A namespace-level banned user can access the API.	2.7	More Details
CVE-2023-4216	The Orders Tracking for WooCommerce WordPress plugin before 1.2.6 doesn't validate the file_url parameter when importing a CSV file, allowing high privilege users with the manage_woocommerce capability to access any file on the web server via a Traversal attack. The content retrieved is however limited to the first line of the file.	2.7	More Details
CVE-2023-1279	An issue has been discovered in GitLab affecting all versions starting from 4.1 before 16.1.5, all versions starting from 16.2 before 16.2.5, all versions starting from 16.3 before 16.3.1 where it was possible to create a URL that would redirect to a different project.	2.6	More Details
CVE-2023-41041	Graylog is a free and open log management platform. In a multi-node Graylog cluster, after a user has explicitly logged out, a user session may still be used for API requests until it has reached its original expiry time. Each node maintains an in-memory cache of user sessions. Upon a cache-miss, the session is loaded from the database. After that, the node operates solely on the cached session. Modifications to sessions will update the cached version as well as the session persisted in the database. However, each node maintains their isolated version of the session. When the user logs out, the session is removed from the node-local cache and deleted from the database. The other nodes will however still use the cached session. These nodes will only fail to accept the session id if they intent to update the session in the database. They will then notice that the session is gone. This is true for most API requests originating from user interaction with the Graylog UI because these will lead to an update of the session's "last access" timestamp. If the session update is however prevented by setting the `X-Graylog-No-Session-Extension:true` header in the request, the node will consider the (cached) session valid until the session is expired according to its timeout setting. No session identifiers are leaked. After a user has logged out, the UI shows the login screen again, which gives the user the impression that their session is not valid anymore. However, if the session becomes compromised later, it can still be used to perform API requests against the Graylog cluster. The time frame for this is limited to the configured session lifetime, starting from the time when the user logged out. This issue has been addressed in versions 5.0.9 and 5.1.3. Users are advised to upgrade.	2.6	More Details
CVE-2023-40184	xrdp is an open source remote desktop protocol (RDP) server. In versions prior to 0.9.23 improper handling of session establishment errors allows bypassing OS-level session restrictions. The `auth_start_session` function can return non-zero (1) value on, e.g., PAM error which may result in in session restrictions such as max concurrent sessions per user by PAM (ex ./etc/security/limits.conf) to be bypassed. Users (administrators) don't use restrictions by PAM are not affected. This issue has been addressed in release version 0.9.23. Users are advised to upgrade. There are no known workarounds for this issue.	2.6	More Details
CVE-2023-41051	In a typical Virtual Machine Monitor (VMM) there are several components, such as boot loader, virtual device drivers, virtio backend drivers and vhost drivers, that need to access the VM physical memory. The vm-memory rust crate provides a set of traits to decouple VM memory consumers from VM memory providers. An issue was discovered in the default implementations of the `VolatileMemory::{get_atomic_ref, aligned_as_ref, aligned_as_mut, get_ref, get_array_ref}` trait functions, which allows out-of-bounds memory access if the `VolatileMemory::get_slice` function returns a `VolatileSlice` whose length is less than the function's `count` argument. No implementations of `get_slice` provided in `vm_memory` are affected. Users of custom `VolatileMemory` implementations may be impacted if the custom implementation does not adhere to `get_slice`'s documentation. The issue started in version 0.1.0 but was fixed in version 0.12.2 by inserting a check that verifies that the `VolatileSlice` returned by `get_slice` is of the correct length. Users are advised to upgrade. There are no known workarounds for this issue.	2.5	More Details
CVE-2023-4624	Server-Side Request Forgery (SSRF) in GitHub repository bookstackapp/bookstack prior to v23.08.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3995	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is a duplicate of CVE-2023-4147.	N/A	More Details
CVE-2023-4525	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-40936	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-40214	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2022. Notes: none.	N/A	More Details
CVE-2023-40937	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-32086	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-4609	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-4526	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-41269	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details