SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 30 August 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-2023-40177	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any registered user can use the content field of their user profile page to execute arbitrary scripts with programming rights, thus effectively performing rights escalation. This issue is present since version 4.3M2 when AppWithinMinutes Application added support for the Content field, allowing any wiki page (including the user profile page) to use its content as an AWM Content field, which has a custom displayer that executes the content with the rights of the ``AppWithinMinutes.Content`` author, rather than the rights of the content author. The vulnerability has been fixed in XWiki 14.10.5 and 15.1RC1. The fix is in the content of the AppWithinMinutes.Content page that defines the custom displayer. By using the ``display`` script service to render the content we make sure that the proper author is used for access rights checks.	9.9	More Details
CVE-2023-4404	The Donation Forms by Charitable plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.7.0.12 due to insufficient restriction on the 'update_core_user' function. This makes it possible for unauthenticated attackers to specify their user role by supplying the 'role' parameter during a registration.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40761	User enumeration is found in PHPJabbers Yacht Listing Script v2.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-38026	SpotCam Co., Ltd. SpotCam FHD 2 has a vulnerability of using hard-coded uBoot credentials. An remote attacker can exploit this vulnerability to access the system to perform arbitrary system operations or disrupt service.	9.8	More Details
CVE-2023-38027	SpotCam Co., Ltd. SpotCam Sense's hidden Telnet function has a vulnerability of OS command injection. An remote unauthenticated attacker can exploit this vulnerability to execute command injection attack to perform arbitrary system commands or disrupt service.	9.8	More Details
CVE-2023-4041	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Out-of-bounds Write, Download of Code Without Integrity Check vulnerability in Silicon Labs Gecko Bootloader on ARM (Firmware Update File Parser modules) allows Code Injection, Authentication Bypass.This issue affects "Standalone" and "Application" versions of Gecko Bootloader.	9.8	More Details
CVE-2023-38029	Saho's attendance devices ADM100 and ADM-100FP has insufficient filtering for special characters and file type within their file uploading function. A unauthenticate remote attacker authenticated can upload and execute arbitrary files to perform arbitrary system commands or disrupt service.	9.8	More Details
CVE-2023-40748	PHPJabbers Food Delivery Script 3.0 has a SQL injection (SQLi) vulnerability in the "q" parameter of index.php.	9.8	More Details
CVE-2023-40749	PHPJabbers Food Delivery Script v3.0 is vulnerable to SQL Injection in the "column" parameter of index.php.	9.8	More Details
CVE-2023-40756	User enumeration is found in PHPJabbers Callback Widget v1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40757	User enumeration is found in PHPJabbers Food Delivery Script v3.1. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40758	User enumeration is found in PHPJabbers Document Creator v1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40759	User enumeration is found in PHP Jabbers Restaurant Booking Script v3.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40760	User enumeration is found in PHP Jabbers Hotel Booking System v4.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40762	User enumeration is found in PHPJabbers Fundraising Script v1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-38024	SpotCam Co., Ltd. SpotCam FHD 2's hidden Telnet function has a vulnerability of using hard-coded Telnet credentials. An remote unauthenticated attacker can exploit this vulnerability to access the system to perform arbitrary system operations or disrupt service.	9.8	More Details
CVE-2023-40763	User enumeration is found in PHPJabbers Taxi Booking Script v2.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40764	User enumeration is found in PHP Jabbers Car Rental Script v3.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40765	User enumeration is found in PHPJabbers Event Booking Calendar v4.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40766	User enumeration is found in in PHPJabbers Ticket Support Script v3.2. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40767	User enumeration is found in in PHPJabbers Make an Offer Widget v1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-40846	Tenda AC6 US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin is vulnerable to Buffer Overflow via function sub_90998.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39560	ECTouch v2 was discovered to contain a SQL injection vulnerability via the $arr['id'] parameter at \default\helpers\insert.php.	9.8	More Details
CVE-2023-41109	SmartNode SN200 (aka SN200) 3.21.2-23021 allows unauthenticated OS Command Injection.	9.8	More Details
CVE-2023-39652	theme volty tvcmsvideotab up to v4.0.0 was discovered to contain a SQL injection vulnerability via the component TvcmsVideoTabConfirmDeleteModuleFrontController::run().	9.8	More Details
CVE-2023-39650	Theme Volty CMS Blog up to version v4.0.1 was discovered to contain a SQL injection vulnerability via the id parameter at /tvcmsblog/single.	9.8	More Details
CVE-2023-38025	SpotCam Co., Ltd. SpotCam FHD 2's hidden Telnet function has a vulnerability of OS command injection. An remote unauthenticated attacker can exploit this vulnerability to execute command injection attack to arbitrary system commands or disrupt service.	9.8	More Details
CVE-2023-40571	weblogic-framework is a tool for detecting weblogic vulnerabilities. Versions 0.2.3 and prior do not verify the returned data packets, and there is a deserialization vulnerability which may lead to remote code execution. When weblogic-framework gets the command echo, it directly deserializes the data returned by the server without verifying it. At the same time, the classloader loads a lot of deserialization calls. In this case, the malicious serialized data returned by the server will cause remote code execution. Version 0.2.4 contains a patch for this issue.	9.8	More Details
CVE-2023-41361	An issue was discovered in FRRouting FRR 9.0. bgpd/bgp_open.c does not check for an overly large length of the rcv software version.	9.8	More Details
CVE-2023-40889	A heap-based buffer overflow exists in the qr_reader_match_centers function of ZBar 0.23.90. Specially crafted QR codes may lead to information disclosure and/or arbitrary code execution. To trigger this vulnerability, an attacker can digitally input the malicious QR code, or prepare it to be physically scanned by the vulnerable scanner.	9.8	More Details
CVE-2020-18912	An issue found in Earcms Ear App v.20181124 allows a remote attacker to execute arbitrary code via the uload/index-uplog.php.	9.8	More Details
CVE-2021-3262	TripSpark VEO Transportation-2.2.x-XP_BB-20201123-184084 NovusEDU-2.2.x-XP_BB-20201123-184084 allows unsafe data inputs in POST body parameters from end users without sanitizing using server-side logic. It was possible to inject custom SQL commands into the "Student Busing Information" search queries.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34039	Aria Operations for Networks contains an Authentication Bypass vulnerability due to a lack of unique cryptographic key generation. A malicious actor with network access to Aria Operations for Networks could bypass SSH authentication to gain access to the Aria Operations for Networks CLI.	9.8	More Details
CVE-2023-40890	A stack-based buffer overflow vulnerability exists in the lookup_sequence function of ZBar 0.23.90. Specially crafted QR codes may lead to information disclosure and/or arbitrary code execution. To trigger this vulnerability, an attacker can digitally input the malicious QR code, or prepare it to be physically scanned by the vulnerable scanner.	9.8	More Details
CVE-2023-39834	PbootCMS below v3.2.0 was discovered to contain a command injection vulnerability via create_function.	9.8	More Details
CVE-2023-40891	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter firewallEn at /goform/SetFirewallCfg.	9.8	More Details
CVE-2023-40892	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter schedStartTime and schedEndTime at /goform/openSchedWifi.	9.8	More Details
CVE-2023-40893	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter time at /goform/PowerSaveSet.	9.8	More Details
CVE-2023-40894	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter list at /goform/SetStaticRouteCfg.	9.8	More Details
CVE-2023-40895	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter list at /goform/SetVirtualServerCfg.	9.8	More Details
CVE-2023-40896	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter list and bindnum at /goform/SetIpMacBind.	9.8	More Details
CVE-2023-40897	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter mac at /goform/GetParentControlInfo.	9.8	More Details
CVE-2023-40898	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter timeZone at /goform/SetSysTimeCfg.	9.8	More Details
CVE-2023-40899	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter macFilterType and parameter deviceList at /goform/setMacFilterCfg.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40900	Tenda AC8 v4 US_AC8V4.0si_V16.03.34.06_cn was discovered to contain a stack overflow via parameter list at /goform/SetNetControlList.	9.8	More Details
CVE-2023-40901	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter macFilterType and parameter deviceList at url /goform/setMacFilterCfg.	9.8	More Details
CVE-2023-40902	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter list and bindnum at /goform/SetIpMacBind.	9.8	More Details
CVE-2023-40904	Tenda AC10 v4 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via parameter macFilterType and parameter deviceList at /goform/setMacFilterCfg.	9.8	More Details
CVE-2023-4419	The LMS5xx uses hard-coded credentials, which potentially allow low-skilled unauthorized remote attackers to reconfigure settings and /or disrupt the functionality of the device.	9.8	More Details
CVE-2023-4420	A remote unprivileged attacker can intercept the communication via e.g. Man-In-The-Middle, due to the absence of Transport Layer Security (TLS) in the SICK LMS5xx. This lack of encryption in the communication channel can lead to the unauthorized disclosure of sensitive information. The attacker can exploit this weakness to eavesdrop on the communication between the LMS5xx and the Client, and potentially manipulate the data being transmitted.	9.8	More Details
CVE-2023-39699	IceWarp Mail Server v10.4.5 was discovered to contain a local file inclusion (LFI) vulnerability via the component /calendar/minimizer/index.php. This vulnerability allows attackers to include or execute files from the local file system of the targeted server.	9.8	More Details
CVE-2023-32757	e-Excellence U-Office Force file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker without logging the service can exploit this vulnerability to upload arbitrary files to perform arbitrary command or disrupt service.	9.8	More Details
CVE-2023-40799	Tenda AC23 Vv16.03.07.45_cn is vulnerable to Buffer Overflow via sub_450A4C function.	9.8	More Details
CVE-2023-40787	In SpringBlade V3.6.0 when executing SQL query, the parameters submitted by the user are not wrapped in quotation marks, which leads to SQL injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41265	An HTTP Request Tunneling vulnerability found in Qlik Sense Enterprise for Windows for versions May 2023 Patch 3 and earlier, February 2023 Patch 7 and earlier, November 2022 Patch 10 and earlier, and August 2022 Patch 12 and earlier allows a remote attacker to elevate their privilege by tunneling HTTP requests in the raw HTTP request. This allows them to send requests that get executed by the backend server hosting the repository application. This is fixed in August 2023 IR, May 2023 Patch 4, February 2023 Patch 8, November 2022 Patch 11, and August 2022 Patch 13.	9.6	More Details
CVE-2019-13690	Inappropriate implementation in OS in Google Chrome on ChromeOS prior to 75.0.3770.80 allowed a remote attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High)	9.6	More Details
CVE-2023-23770	Motorola MBTS Site Controller accepts hard-coded backdoor password. The Motorola MBTS Site Controller Man Machine Interface (MMI), allowing for service technicians to diagnose and configure the device, accepts a hard-coded backdoor password that cannot be changed or disabled.	9.4	More Details
CVE-2023-41360	An issue was discovered in FRRouting FRR through 9.0. bgpd/bgp_packet.c can read the initial byte of the ORF header in an ahead-of-stream situation.	9.1	More Details
CVE-2023-41359	An issue was discovered in FRRouting FRR through 9.0. There is an out-of-bounds read in bgp_attr_aigp_valid in bgpd/bgp_attr.c because there is no check for the availability of two bytes during AIGP validation.	9.1	More Details
CVE-2023-38028	Saho’s attendance devices ADM100 and ADM-100FP have insufficient authentication. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication to read system information and operate user's data, but can’t control system or disrupt service.	9.1	More Details
CVE-2023-40573	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki supports scheduled jobs that contain Groovy scripts. Currently, the job checks the content author of the job for programming right. However, modifying or adding a job script to a document doesn't modify the content author. Together with a CSRF vulnerability in the job scheduler, this can be exploited for remote code execution by an attacker with edit right on the wiki. If the attack is successful, an error log entry with "Job content executed" will be produced. This vulnerability has been patched in XWiki 14.10.9 and 15.4RC1.	9.0	More Details
CVE-2023-40572	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The create action is vulnerable to a CSRF attack, allowing script and thus remote code execution when targeting a user with script/programming right, thus compromising the confidentiality, integrity and availability of the whole XWiki installation. When a user with script right views this image and a log message `ERROR foo - Script executed!` appears in the log, the XWiki installation is vulnerable. This has been patched in XWiki 14.10.9 and 15.4RC1 by requiring a CSRF token for the actual page creation.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41028	A stack-based buffer overflow exists in Juplink RX4-1500, a WiFi router, in versions 1.0.2 through 1.0.5. An authenticated attacker can exploit this vulnerability to achieve code execution as root.	9.0	More Details
CVE-2023-40176	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any registered user can exploit a stored XSS through their user profile by setting the payload as the value of the time zone user preference. Even though the time zone is selected from a drop down (no free text value) it can still be set from JavaScript (using the browser developer tools) or by calling the save URL on the user profile with the right query string. Once the time zone is set it is displayed without escaping which means the payload gets executed for any user that visits the malicious user profile, allowing the attacker to steal information and even gain more access rights (escalation to programming rights). This issue is present since version 4.1M2 when the time zone user preference was introduced. The issue has been fixed in XWiki 14.10.5 and 15.1RC1.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-30435	IBM Security Guardium 11.3, 11.4, and 11.5 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 252291.	8.9	More Details
CVE-2023-40798	In Tenda AC23 v16.03.07.45_cn, the formSetIPv6status and formGetWanParameter functions do not authenticate user input parameters, resulting in a post-authentication stack overflow vulnerability.	8.8	More Details
CVE-2020-24165	An issue was discovered in TCG Accelerator in QEMU 4.2.0, allows local attackers to execute arbitrary code, escalate privileges, and cause a denial of service (DoS). Note: This is disputed as a bug and not a valid security issue by multiple third parties.	8.8	More Details
CVE-2023-32079	Netmaker makes networks with WireGuard. A Mass assignment vulnerability was found in versions prior to 0.17.1 and 0.18.6 that allows a non-admin user to escalate privileges to those of an admin user. The issue is patched in 0.17.1 and fixed in 0.18.6. If Users are using 0.17.1, they should run `docker pull gravitl/netmaker:v0.17.1` and `docker-compose up -d`. This will switch them to the patched users If users are using v0.18.0-0.18.5, they should upgrade to v0.18.6 or later. As a workaround, someone using version 0.17.1 can pull the latest docker image of the backend and restart the server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37469	CasaOS is an open-source personal cloud system. Prior to version 0.4.4, if an authenticated user using CasaOS is able to successfully connect to a controlled SMB server, they are able to execute arbitrary commands. Version 0.4.4 contains a patch for the issue.	8.8	More Details
CVE-2022-4452	Insufficient data validation in crosvm in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-40800	The compare_parentcontrol_time function does not authenticate user input parameters, resulting in a post-authentication stack overflow vulnerability in Tenda AC23 v16.03.07.45_cn.	8.8	More Details
CVE-2023-40801	The sub_451784 function does not validate the parameters entered by the user, resulting in a stack overflow vulnerability in Tenda AC23 v16.03.07.45_cn	8.8	More Details
CVE-2023-40797	In Tenda AC23 v16.03.07.45_cn, the sub_4781A4 function does not validate the parameters entered by the user, resulting in a post-authentication stack overflow vulnerability.	8.8	More Details
CVE-2023-37249	Infoblox NIOS through 8.5.1 has a faulty component that accepts malicious input without sanitization, resulting in shell access.	8.8	More Details
CVE-2023-27604	Apache Airflow Sqoop Provider, versions before 4.0.0, is affected by a vulnerability that allows an attacker pass parameters with the connections, which makes it possible to implement RCE attacks via ‘sqoop import --connect’, obtain airflow server permissions, etc. The attacker needs to be logged in and have authorization (permissions) to create/edit connections. It is recommended to upgrade to a version that is not affected. This issue was reported independently by happyhacking-k, And Xie Jianming and LiuHui of Caiji Sec Team also reported it.	8.8	More Details
CVE-2023-40195	Deserialization of Untrusted Data, Inclusion of Functionality from Untrusted Control Sphere vulnerability in Apache Software Foundation Apache Airflow Spark Provider. When the Apache Spark provider is installed on an Airflow deployment, an Airflow user that is authorized to configure Spark hooks can effectively run arbitrary code on the Airflow node by pointing it at a malicious Spark server. Prior to version 4.1.3, this was not called out in the documentation explicitly, so it is possible that administrators provided authorizations to configure Spark hooks without taking this into account. We recommend administrators to review their configurations to make sure the authorization to configure Spark hooks is only provided to fully trusted users. To view the warning in the docs please visit https://airflow.apache.org/docs/apache-airflow-providers-apache-spark/4.1.3/connections/spark.html	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40754	In PHPJabbers Car Rental Script 3.0, lack of verification when changing an email address and/or password (on the Profile Page) allows remote attackers to take over accounts.	8.8	More Details
CVE-2022-46884	A potential use-after-free vulnerability existed in SVG Images if the Refresh Driver was destroyed at an inopportune time. This could have lead to memory corruption or a potentially exploitable crash. *Note*: This advisory was added on December 13th, 2022 after discovering it was inadvertently left out of the original advisory. The fix was included in the original release of Firefox 106. This vulnerability affects Firefox < 106.	8.8	More Details
CVE-2023-1997	An OS Command Injection vulnerability exists in SIMULIA 3DOrchestrate from Release 3DEXPERIENCE R2021x through Release 3DEXPERIENCE R2023x. A specially crafted HTTP request can lead to arbitrary command execution.	8.8	More Details
CVE-2023-39059	An issue in ansible semaphore v.2.8.90 allows a remote attacker to execute arbitrary code via a crafted payload to the extra variables parameter.	8.8	More Details
CVE-2023-40857	Buffer Overflow vulnerability in VirusTotal yara v.4.3.2 allows a remote attacker to execute arbtirary code via the yr_execute_cod function in the exe.c component.	8.8	More Details
CVE-2023-40144	OS command injection vulnerability in the CBC products allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter its settings. As for the affected products/versions, see the detailed information provided by the vendor. Note that NR4H, NR8H, NR16H series and DR-16F, DR-8F, DR-4F, DR-16H, DR-8H, DR-4H, DR-4M41 series are no longer supported, therefore updates for those products are not provided.	8.8	More Details
CVE-2023-40158	Hidden functionality vulnerability in the CBC products allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter its settings. As for the affected products/versions, see the detailed information provided by the vendor. Note that NR4H, NR8H, NR16H series and DR-16F, DR-8F, DR-4F, DR-16H, DR-8H, DR-4H, DR-4M41 series are no longer supported, therefore updates for those products are not provided.	8.8	More Details
CVE-2023-38585	Improper authentication vulnerability in the CBC products allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter its settings. As for the affected products/versions, see the detailed information provided by the vendor. Note that NR4H, NR8H, NR16H series and DR-16F, DR-8F, DR-4F, DR-16H, DR-8H, DR-4H, DR-4M41 series are no longer supported, therefore updates for those products are not provided.	8.8	More Details
CVE-2023-4572	Use after free in MediaStream in Google Chrome prior to 116.0.5845.140 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-2023-4296	If an attacker tricks an admin user of PTC Codebeamer into clicking on a malicious link, it may allow the attacker to inject arbitrary code to be executed in the browser on the target device.	8.8	More Details
CVE-2023-4430	Use after free in Vulkan in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4429	Use after free in Loader in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-40707	There are no requirements for setting a complex password in the built-in web server of the SNAP PAC S1 Firmware version R10.3b, which could allow for a successful brute force attack if users don't set up complex credentials.	8.6	More Details
CVE-2023-40706	There is no limit on the number of login attempts in the web server for the SNAP PAC S1 Firmware version R10.3b. This could allow for a brute-force attack on the built-in web server login.	8.6	More Details
CVE-2023-23771	Motorola MBTS Base Radio accepts hard-coded backdoor password. The Motorola MBTS Base Radio Man Machine Interface (MMI), allowing for service technicians to diagnose and configure the device, accepts a hard-coded backdoor password that cannot be changed or disabled.	8.4	More Details
CVE-2023-23774	Motorola EBTS/MBTS Site Controller drops to debug prompt on unhandled exception. The Motorola MBTS Site Controller exposes a debug prompt on the device's serial port in case of an unhandled exception. This allows an attacker with physical access that is able to trigger such an exception to extract secret key material and/or gain arbitrary code execution on the device.	8.4	More Details
CVE-2023-36741	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2023-39266	A vulnerability in the ArubaOS-Switch web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface provided certain configuration options are present. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	8.3	More Details
CVE-2023-41266	A path traversal vulnerability found in Qlik Sense Enterprise for Windows for versions May 2023 Patch 3 and earlier, February 2023 Patch 7 and earlier, November 2022 Patch 10 and earlier, and August 2022 Patch 12 and earlier allows an unauthenticated remote attacker to generate an anonymous session. This allows them to transmit HTTP requests to unauthorized endpoints. This is fixed in August 2023 IR, May 2023 Patch 4, February 2023 Patch 8, November 2022 Patch 11, and August 2022 Patch 13.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40580	Freighter is a Stellar chrome extension. It may be possible for a malicious website to access the recovery mnemonic phrase when the Freighter wallet is unlocked. This vulnerability impacts access control to the mnemonic recovery phrase. This issue was patched in version 5.3.1.	8.1	More Details
CVE-2023-4428	Out of bounds memory access in CSS in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2023-4431	Out of bounds memory access in Fonts in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.1	More Details
CVE-2023-35785	Zoho ManageEngine Active Directory 360 versions 4315 and below, ADAudit Plus 7202 and below, ADManager Plus 7200 and below, Asset Explorer 6993 and below and 7xxx 7002 and below, Cloud Security Plus 4161 and below, Data Security Plus 6110 and below, Eventlog Analyzer 12301 and below, Exchange Reporter Plus 5709 and below, Log360 5315 and below, Log360 UEBA 4045 and below, M365 Manager Plus 4529 and below, M365 Security Plus 4529 and below, Recovery Manager Plus 6061 and below, ServiceDesk Plus 14204 and below and 143xx 14302 and below, ServiceDesk Plus MSP 14300 and below, SharePoint Manager Plus 4402 and below, and Support Center Plus 14300 and below are vulnerable to 2FA bypass via a few TOTP authenticators. Note: A valid pair of username and password is required to leverage this vulnerability.	8.1	More Details
CVE-2023-34758	Sliver from v1.5.x to v1.5.39 has an improper cryptographic implementation, which allows attackers to execute a man-in-the-middle attack via intercepted and crafted responses.	8.1	More Details
CVE-2023-4427	Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2023-37379	Apache Airflow, in versions prior to 2.7.0, contains a security vulnerability that can be exploited by an authenticated user possessing Connection edit privileges. This vulnerability allows the user to access connection information and exploit the test connection feature by sending many requests, leading to a denial of service (DoS) condition on the server. Furthermore, malicious actors can leverage this vulnerability to establish harmful connections with the server. Users of Apache Airflow are strongly advised to upgrade to version 2.7.0 or newer to mitigate the risk associated with this vulnerability. Additionally, administrators are encouraged to review and adjust user permissions to restrict access to sensitive functionalities, reducing the attack surface.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40273	The session fixation vulnerability allowed the authenticated user to continue accessing Airflow webserver even after the password of the user has been reset by the admin - up until the expiry of the session of the user. Other than manually cleaning the session database (for database session backend), or changing the secure_key and restarting the webserver, there were no mechanisms to force-logout the user (and all other users with that). With this fix implemented, when using the database session backend, the existing sessions of the user are invalidated when the password of the user is reset. When using the securecookie session backend, the sessions are NOT invalidated and still require changing the secure key and restarting the webserver (and logging out all other users), but the user resetting the password is informed about it with a flash message warning displayed in the UI. Documentation is also updated explaining this behaviour. Users of Apache Airflow are advised to upgrade to version 2.7.0 or newer to mitigate the risk associated with this vulnerability.	8.0	More Details
CVE-2023-39986	** UNSUPPORTED WHEN ASSIGNED ** Out-of-bounds Read vulnerability in Hitachi EH-VIEW (Designer) allows local attackers to potentially disclose information on affected EH-VIEW installations. User interaction is required to exploit the vulnerabilities in that the user must open a malicious file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.8	More Details
CVE-2019-13689	Inappropriate implementation in OS in Google Chrome on ChromeOS prior to 75.0.3770.80 allowed a remote attacker to perform arbitrary read/write via a malicious file. (Chromium security severity: Critical)	7.8	More Details
CVE-2021-27932	Stormshield Network Security (SNS) VPN SSL Client 2.1.0 through 2.8.0 has Insecure Permissions.	7.8	More Details
CVE-2023-24621	An issue was discovered in Esoteric YamlBeans through 1.15. It allows untrusted deserialisation to Java classes by default, where the data and class are controlled by the author of the YAML document being processed.	7.8	More Details
CVE-2023-40031	Notepad++ is a free and open-source source code editor. Versions 8.5.6 and prior are vulnerable to heap buffer write overflow in `Utf8_16_Read::convert`. This issue may lead to arbitrary code execution. As of time of publication, no known patches are available in existing versions of Notepad++.	7.8	More Details
CVE-2023-38831	RARLAB WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The issue occurs because a ZIP archive may include a benign file (such as an ordinary .JPG file) and also a folder that has the same name as the benign file, and the contents of the folder (which may include executable content) are processed during an attempt to access only the benign file. This was exploited in the wild in April through October 2023.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3899	A vulnerability was found in subscription-manager that allows local privilege escalation due to inadequate authorization. The D-Bus interface com.redhat.RHSM1 exposes a significant number of methods to all users that could change the state of the registration. By using the com.redhat.RHSM1.Config.SetAll() method, a low-privileged local user could tamper with the state of the registration, by unregistering the system or by changing the current entitlements. This flaw allows an attacker to set arbitrary configuration directives for /etc/rhsm/rhsm.conf, which can be abused to cause a local privilege escalation to an unconfined root.	7.8	More Details
CVE-2023-40022	Rizin is a UNIX-like reverse engineering framework and command-line toolset. Versions 0.6.0 and prior are vulnerable to integer overflow in `consume_count` of `src/gnu_v2/cplus-dem.c`. The overflow check is valid logic but, is missing the modulus if the block once compiled. The compiler sees this block as unreachable code since the prior statement is multiplication by 10 and fails to consider overflow assuming the count will always be a multiple of 10. Rizin version 0.6.1 contains a fix for the issue. A temporary workaround would be disabling C++ demangling using the configuration option `bin.demangle=false`.	7.8	More Details
CVE-2023-40590	GitPython is a python library used to interact with Git repositories. When resolving a program, Python/Windows look for the current working directory, and after that the PATH environment. GitPython defaults to use the `git` command, if a user runs GitPython from a repo has a `git.exe` or `git` executable, that program will be run instead of the one in the user's `PATH`. This is more of a problem on how Python interacts with Windows systems, Linux and any other OS aren't affected by this. But probably people using GitPython usually run it from the CWD of a repo. An attacker can trick a user to download a repository with a malicious `git` executable, if the user runs/imports GitPython from that directory, it allows the attacker to run any arbitrary commands. There is no fix currently available for windows users, however there are a few mitigations. 1: Default to an absolute path for the git program on Windows, like `C:\\Program Files\\Git\\cmd\\git.EXE` (default git path installation). 2: Require users to set the `GIT_PYTHON_GIT_EXECUTABLE` environment variable on Windows systems. 3: Make this problem prominent in the documentation and advise users to never run GitPython from an untrusted repo, or set the `GIT_PYTHON_GIT_EXECUTABLE` env var to an absolute path. 4: Resolve the executable manually by only looking into the `PATH` environment variable.	7.8	More Details
CVE-2023-39810	An issue in the CPIO command of Busybox v1.33.2 allows attackers to execute a directory traversal.	7.8	More Details
CVE-2023-41005	An issue in Pagekit pagekit v.1.0.18 alows a remote attacker to execute arbitrary code via thedownloadAction and updateAction functions in UpdateController.php	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3495	** UNSUPPORTED WHEN ASSIGNED ** Out-of-bounds Write vulnerability in Hitachi EH-VIEW (KeypadDesigner) allows local attackers to potentially execute arbitray code on affected EH-VIEW installations. User interaction is required to exploit the vulnerabilities in that the user must open a malicious file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.8	More Details
CVE-2023-40796	Phicomm k2 v22.6.529.216 was discovered to contain a command injection vulnerability via the function luci.sys.call.	7.8	More Details
CVE-2023-39984	** UNSUPPORTED WHEN ASSIGNED ** Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Hitachi EH-VIEW (KeypadDesigner) allows local attackers to potentially disclose information and execute arbitray code on affected EH-VIEW installations. User interaction is required to exploit the vulnerabilities in that the user must open a malicious file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.8	More Details
CVE-2023-39985	** UNSUPPORTED WHEN ASSIGNED ** Out-of-bounds Write vulnerability in Hitachi EH-VIEW (Designer) allows local attackers to potentially execute arbitray code on affected EH-VIEW installations. User interaction is required to exploit the vulnerabilities in that the user must open a malicious file. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.8	More Details
CVE-2023-20200	A vulnerability in the Simple Network Management Protocol (SNMP) service of Cisco FXOS Software for Firepower 4100 Series and Firepower 9300 Security Appliances and of Cisco UCS 6300 Series Fabric Interconnects could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to the improper handling of specific SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: This vulnerability affects all supported SNMP versions. To exploit this vulnerability through SNMPv2c or earlier, an attacker must know the SNMP community string that is configured on an affected device. To exploit this vulnerability through SNMPv3, the attacker must have valid credentials for an SNMP user who is configured on the affected device.	7.7	More Details
CVE-2023-3406	Path Traversal issue in M-Files Classic Web versions below 23.6.12695.3 and LTS Service Release Versions before 23.2 LTS SR3 allows authenticated user to read some restricted files on the web server	7.7	More Details
CVE-2023-33852	IBM Security Guardium 11.4 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 257614.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4346	KNX devices that use KNX Connection Authorization and support Option 1 are, depending on the implementation, vulnerable to being locked and users being unable to reset them to gain access to the device. The BCU key feature on the devices can be used to create a password for the device, but this password can often not be reset without entering the current password. If the device is configured to interface with a network, an attacker with access to that network could interface with the KNX installation, purge all devices without additional security options enabled, and set a BCU key, locking the device. Even if a device is not connected to a network, an attacker with physical access to the device could also exploit this vulnerability in the same way.	7.5	More Details
CVE-2023-4418	A remote unprivileged attacker can sent multiple packages to the LMS5xx to disrupt its availability through a TCP SYN-based denial-of-service (DDoS) attack. By exploiting this vulnerability, an attacker can flood the targeted LMS5xx with a high volume of TCP SYN requests, overwhelming its resources and causing it to become unresponsive or unavailable for legitimate users.	7.5	More Details
CVE-2023-39289	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect through 9.6.2208.101 could allow an unauthenticated attacker to conduct an account enumeration attack due to improper configuration. A successful exploit could allow an attacker to access system information.	7.5	More Details
CVE-2023-41121	Array AG OS before 9.4.0.499 allows denial of service: remote attackers can cause system service processes to crash through abnormal HTTP operations.	7.5	More Details
CVE-2023-36198	Buffer Overflow vulnerability in skalenetwork sgxwallet v.1.9.0 allows an attacker to cause a denial of service via the trustedBlsSignMessage function.	7.5	More Details
CVE-2023-40599	Regular expression Denial-of-Service (ReDoS) exists in multiple add-ons for Mailform Pro CGI 4.3.1.3 and earlier, which allows a remote unauthenticated attacker to cause a denial-of-service condition. Affected add-ons are as follows: call/call.js, prefcodeadv/search.cgi, estimate/estimate.js, search/search.js, suggest/suggest.js, and coupon/coupon.js.	7.5	More Details
CVE-2023-39663	Mathjax up to v2.7.9 was discovered to contain two Regular expression Denial of Service (ReDoS) vulnerabilities in MathJax.js via the components pattern and markdownPattern. NOTE: the vendor disputes this because the regular expressions are not applied to user input; thus, there is no risk.	7.5	More Details
CVE-2023-40577	Alertmanager handles alerts sent by client applications such as the Prometheus server. An attacker with the permission to perform POST requests on the /api/v1/alerts endpoint could be able to execute arbitrary JavaScript code on the users of Prometheus Alertmanager. This issue has been fixed in Alertmanager version 0.2.51.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40915	Tenda AX3 v16.03.12.11 has a stack buffer overflow vulnerability detected at function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ssid parameter.	7.5	More Details
CVE-2023-31412	The LMS5xx uses weak hash generation methods, resulting in the creation of insecure hashs. If an attacker manages to retrieve the hash, it could lead to collision attacks and the potential retrieval of the password.	7.5	More Details
CVE-2023-32077	Netmaker makes networks with WireGuard. Prior to versions 0.17.1 and 0.18.6, hardcoded DNS key usage has been found in Netmaker allowing unauth users to interact with DNS API endpoints. The issue is patched in 0.17.1 and fixed in 0.18.6. If users are using 0.17.1, they should run `docker pull gravitl/netmaker:v0.17.1` and `docker-compose up -d`. This will switch them to the patched users. If users are using v0.18.0-0.18.5, they should upgrade to v0.18.6 or later. As a workaround, someone who is using version 0.17.1 can pull the latest docker image of the backend and restart the server.	7.5	More Details
CVE-2023-41105	An issue was discovered in Python 3.11 through 3.11.4. If a path containing '\0' bytes is passed to os.path.normpath(), the path will be truncated unexpectedly at the first '\0' byte. There are plausible cases in which an application would have rejected a filename for security reasons in Python 3.10.x or earlier, but that filename is no longer rejected in Python 3.11.x.	7.5	More Details
CVE-2022-43904	IBM Security Guardium 11.3 and 11.4 could disclose sensitive information to an attacker due to improper restriction of excessive authentication attempts. IBM X-Force ID: 240895.	7.5	More Details
CVE-2023-32078	Netmaker makes networks with WireGuard. An Insecure Direct Object Reference (IDOR) vulnerability was found in versions prior to 0.17.1 and 0.18.6 in the user update function. By specifying another user's username, it was possible to update the other user's password. The issue is patched in 0.17.1 and fixed in 0.18.6. If Users are using 0.17.1, they should run `docker pull gravitl/netmaker:v0.17.1` and `docker-compose up -d`. This will switch them to the patched users. If users are using v0.18.0-0.18.5, they should upgrade to v0.18.6 or later. As a workaround, someone using version 0.17.1 can pull the latest docker image of the backend and restart the server.	7.5	More Details
CVE-2023-36481	An issue was discovered in Samsung Exynos Mobile Processor and Wearable Processor 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, and W920. Improper handling of PPP length parameter inconsistency can cause an infinite loop.	7.5	More Details
CVE-2023-36199	An issue in skalenetwork sgxwallet v.1.9.0 and below allows an attacker to cause a denial of service via the trustedGenerateEcdsaKey component.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39519	Cloud Explorer Lite is an open source cloud management platform. Prior to version 1.4.0, there is a risk of sensitive information leakage in the user information acquisition of CloudExplorer Lite. The vulnerability has been fixed in version 1.4.0.	7.5	More Details
CVE-2023-26095	ASQ in Stormshield Network Security (SNS) 4.3.15 before 4.3.16 and 4.6.x before 4.6.3 allows a crash when analysing a crafted SIP packet.	7.5	More Details
CVE-2023-40017	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. In versions 3.2.0 through 4.1.2, the endpoint `/proxy/?url=` does not properly protect against server-side request forgery. This allows an attacker to port scan internal hosts and request information from internal hosts. A patch is available at commit a9eebae80cb362009660a1fd49e105e7cdb499b9.	7.5	More Details
CVE-2023-38030	Saho's attendance devices ADM100 and ADM-100FP have a vulnerability of missing authentication for critical functions. An unauthenticated remote attacker can execute system commands in partial website URLs to read sensitive device information without permissions.	7.5	More Details
CVE-2023-38975	* Buffer Overflow vulnerability in qdrant v.1.3.2 allows a remote attacker cause a denial of service via the chucnked_vectors.rs component.	7.5	More Details
CVE-2023-40826	An issue in pf4j pf4j v.3.9.0 and before allows a remote attacker to obtain sensitive information and execute arbitrary code via the zippluginPath parameter.	7.5	More Details
CVE-2023-40827	An issue in pf4j pf4j v.3.9.0 and before allows a remote attacker to obtain sensitive information and execute arbitrary code via the loadpluginPath parameter.	7.5	More Details
CVE-2023-3705	The vulnerability exists in CP-Plus NVR due to an improper input handling at the web-based management interface of the affected product. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable device. Successful exploitation of this vulnerability could allow the remote attacker to obtain sensitive information on the targeted device.	7.5	More Details
CVE-2023-38422	Walchem Intuition 9 firmware versions prior to v4.21 are missing authentication for some of the API routes of the management web server. This could allow an attacker to download and export sensitive data.	7.5	More Details
CVE-2023-41376	Nokia Service Router Operating System (SR OS) 22.10 and SR Linux, when error-handling update-fault-tolerance is not enabled, mishandle BGP path attributes.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40586	OWASP Coraza WAF is a golang modsecurity compatible web application firewall library. Due to the misuse of `log.Fatalf`, the application using coraza crashed after receiving crafted requests from attackers. The application will immediately crash after receiving a malicious request that triggers an error in `mime.ParseMediaType`. This issue was patched in version 3.0.1.	7.5	More Details
CVE-2023-32457	Dell PowerScale OneFS, versions 8.2.2.x-9.5.0.x, contains an improper privilege management vulnerability. A remote attacker with low privileges could potentially exploit this vulnerability, leading to escalation of privileges.	7.5	More Details
CVE-2023-41358	An issue was discovered in FRRouting FRR through 9.0. bgpd/bgp_packet.c processes NLRIs if the attribute length is zero.	7.5	More Details
CVE-2023-40583	libp2p is a networking stack and library modularized out of The IPFS Project, and bundled separately for other tools to use. In go-libp2p, by using signed peer records a malicious actor can store an arbitrary amount of data in a remote node's memory. This memory does not get garbage collected and so the victim can run out of memory and crash. If users of go-libp2p in production are not monitoring memory consumption over time, it could be a silent attack i.e. the attacker could bring down nodes over a period of time (how long depends on the node resources i.e. a go-libp2p node on a virtual server with 4 gb of memory takes about 90 sec to bring down; on a larger server, it might take a bit longer.) This issue was patched in version 0.27.4.	7.5	More Details
CVE-2023-39616	AOMedia v3.0.0 to v3.5.0 was discovered to contain an invalid read memory access via the component assign_frame_buffer_p in av1/common/av1_common_int.h.	7.5	More Details
CVE-2023-32559	A privilege escalation vulnerability exists in the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. The use of the deprecated API `process.binding()` can bypass the policy mechanism by requiring internal modules and eventually take advantage of `process.binding('spawn_sync')` run arbitrary code, outside of the limits defined in a `policy.json` file. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.	7.5	More Details
CVE-2023-40998	Buffer Overflow vulnerability in O-RAN Software Community ric-plt-lib-rmr v.4.9.0 allows a remote attacker to cause a denial of service via the packet size component.	7.5	More Details
CVE-2023-32756	e-Excellence U-Office Force has a path traversal vulnerability within its file uploading and downloading functions. An unauthenticated remote attacker can exploit this vulnerability to read arbitrary system files, but can't control system or disrupt service.	7.5	More Details
CVE-2023-41173	AdGuard DNS before 2.2 allows remote attackers to cause a denial of service via malformed UDP packets.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34723	An issue was discovered in TechView LA-5570 Wireless Gateway 1.0.19_T53, allows attackers to gain sensitive information via /config/system.conf.	7.5	More Details
CVE-2023-40997	Buffer Overflow vulnerability in O-RAN Software Community ric-plt-lib-rmr v.4.9.0 allows a remote attacker to cause a denial of service via a crafted packet.	7.5	More Details
CVE-2023-40828	An issue in pf4j pf4j v.3.9.0 and before allows a remote attacker to obtain sensitive information and execute arbitrary code via the expandIfZip method in the extract function.	7.5	More Details
CVE-2023-38802	FRRouting FRR 7.5.1 through 9.0 and Pica8 PICOS 4.3.3.2 allow a remote attacker to cause a denial of service via a crafted BGP update with a corrupted attribute 23 (Tunnel Encapsulation).	7.5	More Details
CVE-2023-20169	A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco NX-OS Software for the Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload. This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the unexpected restart of the IS-IS process, which could cause the affected device to reload. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2 adjacent to the affected device.	7.4	More Details
CVE-2023-40585	ironic-image is a container image to run OpenStack Ironic as part of Metal³. Prior to version capm3-v1.4.3, if Ironic is not deployed with TLS and it does not have API and Conductor split into separate services, access to the API is not protected by any authentication. Ironic API is also listening in host network. In case the node is not behind a firewall, the API could be accessed by anyone via network without authentication. By default, Ironic API in Metal3 is protected by TLS and basic authentication, so this vulnerability requires operator to configure API without TLS for it to be vulnerable. TLS and authentication however should not be coupled as they are in versions prior to capm3-v1.4.3. A patch exists in versions capm3-v1.4.3 and newer. Some workarounds are available. Either configure TLS for Ironic API (`deploy.sh -t ...`, `IRONIC_TLS_SETUP=true`) or split Ironic API and Conductor via configuration change (old implementation, not recommended). With both workarounds, services are configured with httpd front-end, which has proper authentication configuration in place.	7.3	More Details
CVE-2022-43907	IBM Security Guardium 11.4 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 240901.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41362	MyBB before 1.8.36 allows Code Injection by users with certain high privileges. Templates in Admin CP intentionally use eval, and there was some validation of the input to eval, but type juggling interfered with this when using PCRE within PHP.	7.2	More Details
CVE-2023-23773	Motorola EBTS/MBTS Base Radio fails to check firmware authenticity. The Motorola MBTS Base Radio lacks cryptographic signature validation for firmware update packages, allowing an authenticated attacker to gain arbitrary code execution, extract secret key material, and/or leave a persistent implant on the device.	7.2	More Details
CVE-2023-40825	An issue in Perfree PerfreeBlog v.3.1.2 allows a remote attacker to execute arbitrary code via crafted plugin listed in admin/plugin/access/list.	7.2	More Details
CVE-2023-20890	Aria Operations for Networks contains an arbitrary file write vulnerability. An authenticated malicious actor with administrative access to VMware Aria Operations for Networks can write files to arbitrary locations resulting in remote code execution.	7.2	More Details
CVE-2023-40035	Craft is a CMS for creating custom digital experiences on the web and beyond. Bypassing the validatePath function can lead to potential remote code execution. This vulnerability can lead to malicious control of vulnerable systems and data exfiltrations. Although the vulnerability is exploitable only in the authenticated users, configuration with ALLOW_ADMIN_CHANGES=true, there is still a potential security threat (Remote Code Execution). This issue has been patched in version 4.4.15 and version 3.8.15.	7.2	More Details
CVE-2023-23772	Motorola MBTS Site Controller fails to check firmware update authenticity. The Motorola MBTS Site Controller lacks cryptographic signature validation for firmware update packages, allowing an authenticated attacker to gain arbitrary code execution, extract secret key material, and/or leave a persistent implant on the device.	7.2	More Details
CVE-2023-32236	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Booking Ultra Pro Booking Ultra Pro Appointments Booking Calendar Plugin <= 1.1.8 versions.	7.1	More Details
CVE-2023-32518	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ono Oogami WP Chinese Conversion plugin <= 1.1.16 versions.	7.1	More Details
CVE-2023-32603	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RedNao Donations Made Easy – Smart Donations plugin <= 4.0.12 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20168	A vulnerability in TACACS+ and RADIUS remote authentication for Cisco NX-OS Software could allow an unauthenticated, local attacker to cause an affected device to unexpectedly reload. This vulnerability is due to incorrect input validation when processing an authentication attempt if the directed request option is enabled for TACACS+ or RADIUS. An attacker could exploit this vulnerability by entering a crafted string at the login prompt of an affected device. A successful exploit could allow the attacker to cause the affected device to unexpectedly reload, resulting in a denial of service (DoS) condition.	7.1	More Details
CVE-2023-32300	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Yoast Yoast SEO: Local plugin <= 14.8 versions.	7.1	More Details
CVE-2023-32598	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in A. R. Jones Featured Image Pro Post Grid plugin <= 5.14 versions.	7.1	More Details
CVE-2023-32509	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Rolf van Gelder Order Your Posts Manually plugin <= 2.2.5 versions.	7.1	More Details
CVE-2023-32797	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution video carousel slider with lightbox plugin <= 1.0.22 versions.	7.1	More Details
CVE-2023-34971	An inadequate encryption strength vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows local network clients to decrypt the data using brute force attacks via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later QuTS hero h5.1.0.2424 build 20230609 and later QuTS hero h4.5.4.2476 build 20230728 and later	7.1	More Details
CVE-2023-32241	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPDeveloper Essential Addons for Elementor Pro plugin <= 5.4.8 versions.	7.1	More Details
CVE-2023-32516	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in GloriaFood Restaurant Menu – Food Ordering System – Table Reservation plugin <= 2.3.6 versions.	7.1	More Details
CVE-2023-32511	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Booking Ultra Pro Booking Ultra Pro Appointments Booking Calendar Plugin plugin <= 1.1.8 versions.	7.1	More Details
CVE-2023-32510	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Rolf van Gelder Order Your Posts Manually plugin <= 2.2.5 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28994	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in UX-themes Flatsome plugin <= 3.16.8 versions.	7.1	More Details
CVE-2023-3453	ETIC Telecom RAS versions 4.7.0 and prior the web management portal authentication disabled by default. This could allow an attacker with adjacent network access to alter the configuration of the device or cause a denial-of-service condition.	7.1	More Details
CVE-2023-32499	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Tony Zeoli, Tony Hayes Radio Station by netmix® – Manage and play your Show Schedule in WordPress! plugin <= 2.4.0.9 versions.	7.1	More Details
CVE-2023-22877	IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 244368.	7.0	More Details
CVE-2023-4611	A use-after-free flaw was found in mm/mempolicy.c in the memory management subsystem in the Linux Kernel. This issue is caused by a race between mbind() and VMA-locked page fault, and may allow a local attacker to crash the system or lead to a kernel information leak.	7.0	More Details
CVE-2023-25649	There is a command injection vulnerability in a mobile internet product of ZTE. Due to insufficient validation of SET_DEVICE_LED interface parameter, an authenticated attacker could use the vulnerability to execute arbitrary commands.	6.8	More Details
CVE-2023-40710	An adversary could cause a continuous restart loop to the entire device by sending a large quantity of HTTP GET requests if the controller has the built-in web server enabled but does not have the built-in web server completely set up and configured for the SNAP PAC S1 Firmware version R10.3b	6.8	More Details
CVE-2023-34724	An issue was discovered in TECHView LA5570 Wireless Gateway 1.0.19_T53, allows physical attackers to gain escalated privileges via the UART interface.	6.8	More Details
CVE-2023-3252	An arbitrary file write vulnerability exists where an authenticated, remote attacker with administrator privileges could alter logging variables to overwrite arbitrary files on the remote host with log data, which could lead to a denial of service condition.	6.8	More Details
CVE-2023-40709	An adversary could crash the entire device by sending a large quantity of ICMP requests if the controller has the built-in web server enabled but does not have the built-in web server completely set up and configured for the SNAP PAC S1 Firmware version R10.3b	6.8	More Details
CVE-2023-34725	An issue was discovered in TechView LA-5570 Wireless Gateway 1.0.19_T53, allows physical attackers to gain escalated privileges via a telnet connection.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3746	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to cause some peripherals to work abnormally due to an exposed Embedded Controller (EC) interface.	6.7	More Details
CVE-2022-3744	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to unlock UEFI variables due to a hard-coded SMI handler credential.	6.7	More Details
CVE-2022-3742	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to execute arbitrary code due to improper buffer validation.	6.7	More Details
CVE-2023-39267	An authenticated remote code execution vulnerability exists in the command line interface in ArubaOS-Switch. Successful exploitation results in a Denial-of-Service (DoS) condition in the switch.	6.6	More Details
CVE-2023-39615	Xmlsoft Libxml2 v2.11.0 was discovered to contain an out-of-bounds read via the xmlSAX2StartElement() function at /libxml2/SAX2.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via supplying a crafted XML file. NOTE: the vendor's position is that the product does not support the legacy SAX1 interface with custom callbacks; there is a crash even without crafted input.	6.5	More Details
CVE-2023-38201	A flaw was found in the Keylime registrar that could allow a bypass of the challenge-response protocol during agent registration. This issue may allow an attacker to impersonate an agent and hide the true status of a monitored machine if the fake agent is added to the verifier list by a legitimate user, resulting in a breach of the integrity of the registrar database.	6.5	More Details
CVE-2023-40781	Buffer Overflow vulnerability in Libming Libming v.0.4.8 allows a remote attacker to cause a denial of service via a crafted .swf file to the makeswf function.	6.5	More Details
CVE-2023-38711	An issue was discovered in Libreswan before 4.12. When an IKEv1 Quick Mode connection configured with ID_IPV4_ADDR or ID_IPV6_ADDR receives an IDcr payload with ID_FQDN, a NULL pointer dereference causes a crash and restart of the pluto daemon. NOTE: the earliest affected version is 4.6.	6.5	More Details
CVE-2023-38712	An issue was discovered in Libreswan 3.x and 4.x before 4.12. When an IKEv1 ISAKMP SA Informational Exchange packet contains a Delete/Notify payload followed by further Notifies that act on the ISAKMP SA, such as a duplicated Delete/Notify message, a NULL pointer dereference on the deleted state causes the pluto daemon to crash and restart.	6.5	More Details
CVE-2023-4560	Improper Authorization of Index Containing Sensitive Information in GitHub repository omeka/omeka-s prior to 4.0.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40579	OpenFGA is an authorization/permission engine built for developers and inspired by Google Zanzibar. Some end users of OpenFGA v1.3.0 or earlier are vulnerable to authorization bypass when calling the ListObjects API. The vulnerability affects customers using `ListObjects` with specific models. The affected models contain expressions of type `rel1 from type1`. This issue has been patched in version 1.3.1.	6.5	More Details
CVE-2023-2906	Due to a failure in validating the length provided by an attacker-crafted CP2179 packet, Wireshark versions 2.0.0 through 4.0.7 is susceptible to a divide by zero allowing for a denial of service attack.	6.5	More Details
CVE-2023-32678	Zulip is an open-source team collaboration tool with topic-based threading that combines email and chat. Users who used to be subscribed to a private stream and have been removed from it since retain the ability to edit messages/topics, move messages to other streams, and delete messages that they used to have access to, if other relevant organization permissions allow these actions. For example, a user may be able to edit or delete their old messages they posted in such a private stream. An administrator will be able to delete old messages (that they had access to) from the private stream. This issue was fixed in Zulip Server version 7.3.	6.5	More Details
CVE-2023-26270	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3)) could allow a remote attacker to execute arbitrary code on the system, caused by an angular template injection flaw. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 248119.	6.5	More Details
CVE-2023-41104	libvmod-digest before 1.0.3, as used in Varnish Enterprise 6.0.x before 6.0.11r5, has an out-of-bounds memory access during base64 decoding, leading to both authentication bypass and information disclosure; however, the exact attack surface will depend on the particular VCL (Varnish Configuration Language) configuration in use.	6.5	More Details
CVE-2023-38710	An issue was discovered in Libreswan before 4.12. When an IKEv2 Child SA REKEY packet contains an invalid IPsec protocol ID number of 0 or 1, an error notify INVALID_SPI is sent back. The notify payload's protocol ID is copied from the incoming packet, but the code that verifies outgoing packets fails an assertion that the protocol ID must be ESP (2) or AH(3) and causes the pluto daemon to crash and restart. NOTE: the earliest affected version is 3.20.	6.5	More Details
CVE-2023-40802	The get_parentControl_list_Info function does not verify the parameters entered by the user, causing a post-authentication heap overflow vulnerability in Tenda AC23 v16.03.07.45_cn	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38508	Tuleap is an open source suite to improve management of software developments and collaboration. In Tuleap Community Edition prior to version 14.11.99.28 and Tuleap Enterprise Edition prior to versions 14.10-6 and 14.11-3, the preview of an artifact link with a type does not respect the project, tracker and artifact level permissions. The issue occurs on the artifact view (not reproducible on the artifact modal). Users might get access to information they should not have access to. Only the title, status, assigned to and last update date fields as defined by the semantics are impacted. If those fields have strict permissions (e.g. the title is only visible to a specific user group) those permissions are still enforced. Tuleap Community Edition 14.11.99.28, Tuleap Enterprise Edition 14.10-6, and Tuleap Enterprise Edition 14.11-3 contain a fix for this issue.	6.5	More Details
CVE-2023-32576	Auth. (subscriber+) Stored Cross-Site Scripting') vulnerability in Plainware Locatoraid Store Locator plugin <= 3.9.18 versions.	6.5	More Details
CVE-2023-40185	shescape is simple shell escape library for JavaScript. This may impact users that use Shescape on Windows in a threaded context. The vulnerability can result in Shescape escaping (or quoting) for the wrong shell, thus allowing attackers to bypass protections depending on the combination of expected and used shell. This bug has been patched in version 1.7.4.	6.5	More Details
CVE-2023-32202	Walchem Intuition 9 firmware versions prior to v4.21 are vulnerable to improper authentication. Login credentials are stored in a format that could allow an attacker to use them as-is to login and gain access to the device.	6.5	More Details
CVE-2023-3425	Out-of-bounds read issue in M-Files Server versions below 23.8.12892.6 and LTS Service Release Versions before 23.2 LTS SR3 allows unauthenticated user to read restricted amount of bytes from memory.	6.5	More Details
CVE-2023-25981	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ThemeKraft Post Form plugin <= 2.8.1 versions.	6.5	More Details
CVE-2023-4543	A vulnerability was found in IBOS OA 4.5.5. It has been declared as critical. This vulnerability affects unknown code of the file ?r=recruit/contact/export&contactids=x. The manipulation 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-238048. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4545	A vulnerability was found in IBOS OA 4.5.5. It has been classified as critical. Affected is an unknown function of the file ?r=recruit/bgchecks/export&checkids=x. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-238056. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4548	A vulnerability classified as critical has been found in SPA-Cart eCommerce CMS 1.9.0.3. This affects an unknown part of the file /search of the component GET Parameter Handler. The manipulation of the argument filter[brandid] leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-238059.	6.3	More Details
CVE-2023-4556	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. Affected by this issue is the function mysqli_query of the file sexit.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-238154 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4557	A vulnerability classified as critical has been found in SourceCodester Inventory Management System 1.0. Affected is an unknown function of the file app/ajax/search_purchase_paymen_report.php. The manipulation of the argument customer leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-238158 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4558	A vulnerability classified as critical was found in SourceCodester Inventory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file staff_data.php. The manipulation of the argument columns[0][data] leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-238159.	6.3	More Details
CVE-2023-4559	A vulnerability, which was classified as critical, has been found in Bettershop LaikeTui. Affected by this issue is some unknown functionality of the file index.php?module=api&action=user&m=upload of the component POST Request Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-238160.	6.3	More Details
CVE-2023-4542	A vulnerability was found in D-Link DAR-8000-10 up to 20230809. It has been classified as critical. This affects an unknown part of the file /app/sys1.php. The manipulation of the argument cmd with the input id leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-238047. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-40371	IBM AIX 7.2, 7.3, VIOS 3.1's OpenSSH implementation could allow a non-privileged local user to access files outside of those allowed due to improper access controls. IBM X-Force ID: 263476.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39600	IceWarp 11.4.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the color parameter.	6.1	More Details
CVE-2020-27366	Cross Site Scripting (XSS) vulnerability in wlscanresults.html in Humax HGB10R-02 BRGCAB version 1.0.03, allows local attackers to execute arbitrary code.	6.1	More Details
CVE-2023-39558	AudimexEE v15.0 was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities via the Show Kai Data component.	6.1	More Details
CVE-2023-39678	A cross-site scripting (XSS) vulnerability in the device web interface (Log Query page) of BDCOM OLT P3310D-2AC 10.1.0F Build 69083 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter.	6.1	More Details
CVE-2023-41098	An issue was discovered in MISP 2.4.174. In app/Controller/DashboardsController.php, a reflected XSS issue exists via the id parameter upon a dashboard edit.	6.1	More Details
CVE-2023-39709	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 Member section.	6.1	More Details
CVE-2023-41080	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92. The vulnerability is limited to the ROOT (default) web application.	6.1	More Details
CVE-2023-39062	Cross Site Scripting vulnerability in Spipu HTML2PDF before v.5.2.8 allows a remote attacker to execute arbitrary code via a crafted script to the forms.php.	6.1	More Details
CVE-2023-39708	A stored cross-site scripting (XSS) vulnerability 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 Add New parameter under the New Buy section.	6.1	More Details
CVE-2023-40755	There is a Cross Site Scripting (XSS) vulnerability in the "theme" parameter of preview.php in PHPJabbers Callback Widget v1.0.	6.1	More Details
CVE-2023-39700	IceWarp Mail Server v10.4.5 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the color parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40030	Cargo downloads a Rust project’s dependencies and compiles the project. Starting in Rust 1.60.0 and prior to 1.72, Cargo did not escape Cargo feature names when including them in the report generated by `cargo build --timings`. A malicious package included as a dependency may inject nearly arbitrary HTML here, potentially leading to cross-site scripting if the report is subsequently uploaded somewhere. The vulnerability affects users relying on dependencies from git, local paths, or alternative registries. Users who solely depend on crates.io are unaffected. Rust 1.60.0 introduced `cargo build --timings`, which produces a report of how long the different steps of the build process took. It includes lists of Cargo features for each crate. Prior to Rust 1.72, Cargo feature names were allowed to contain almost any characters (with some exceptions as used by the feature syntax), but it would produce a future incompatibility warning about them since Rust 1.49. crates.io is far more stringent about what it considers a valid feature name and has not allowed such feature names. As the feature names were included unescaped in the timings report, they could be used to inject Javascript into the page, for example with a feature name like `features = ["<img src='' onerror=alert(0)"]`. If this report were subsequently uploaded to a domain that uses credentials, the injected Javascript could access resources from the website visitor. This issue was fixed in Rust 1.72 by turning the future incompatibility warning into an error. Users should still exercise care in which package they download, by only including trusted dependencies in their projects. Please note that even with these vulnerabilities fixed, by design Cargo allows arbitrary code execution at build time thanks to build scripts and procedural macros: a malicious dependency will be able to cause damage regardless of these vulnerabilities. crates.io has server-side checks preventing this attack, and there are no packages on crates.io exploiting these vulnerabilities. crates.io users still need to excercise care in choosing their dependencies though, as remote code execution is allowed by design there as well.	6.1	More Details
CVE-2023-40752	There is a Cross Site Scripting (XSS) vulnerability in the "action" parameter of index.php in PHPJabbers Make an Offer Widget v1.0.	6.1	More Details
CVE-2023-40750	There is a Cross Site Scripting (XSS) vulnerability in the "action" parameter of index.php in PHPJabbers Yacht Listing Script v1.0.	6.1	More Details
CVE-2023-40751	PHPJabbers Fundraising Script v1.0 is vulnerable to Cross Site Scripting (XSS) via the "action" parameter of index.php.	6.1	More Details
CVE-2023-38730	IBM Storage Copy Data Management 2.2.0.0 through 2.2.19.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 262268.	5.9	More Details
CVE-2023-3646	On affected platforms running Arista EOS with mirroring to multiple destinations configured, an internal system error may trigger a kernel panic and cause system reload.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32505	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Arshid Easy Hide Login plugin <= 1.0.7 versions.	5.9	More Details
CVE-2023-32577	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eji Osigwe DevBuddy Twitter Feed plugin <= 4.0.0 versions.	5.9	More Details
CVE-2023-32584	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in John Newcombe eBecas plugin <= 3.1.3 versions.	5.9	More Details
CVE-2023-32595	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Palasthotel by Edward Bock, Katharina Rompf Sunny Search plugin <= 1.0.2 versions.	5.9	More Details
CVE-2023-39441	Apache Airflow SMTP Provider before 1.3.0, Apache Airflow IMAP Provider before 3.3.0, and Apache Airflow before 2.7.0 are affected by the Validation of OpenSSL Certificate vulnerability. The default SSL context with SSL library did not check a server's X.509 certificate. Instead, the code accepted any certificate, which could result in the disclosure of mail server credentials or mail contents when the client connects to an attacker in a MITM position. Users are strongly advised to upgrade to Apache Airflow version 2.7.0 or newer, Apache Airflow IMAP Provider version 3.3.0 or newer, and Apache Airflow SMTP Provider version 1.3.0 or newer to mitigate the risk associated with this vulnerability	5.9	More Details
CVE-2023-32575	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PI Websolution Product page shipping calculator for WooCommerce plugin <= 1.3.25 versions.	5.9	More Details
CVE-2023-32591	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Cloud Primero B.V DBargain plugin <= 3.0.0 versions.	5.9	More Details
CVE-2023-24394	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy iframe popup plugin <= 3.3 versions.	5.9	More Details
CVE-2023-32496	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bill Minozzi Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection plugin <= 7.31 versions.	5.9	More Details
CVE-2023-32498	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Easy Form team Easy Form by AYS plugin <= 1.2.0 versions.	5.9	More Details
CVE-2023-32596	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wolfgang Ertl weebotLite plugin <= 1.0.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32119	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPO365	Mail Integration for Office 365 / Outlook plugin <= 1.9.0 versions.	5.8	More Details
CVE-2023-40708	The File Transfer Protocol (FTP) port is open by default in the SNAP PAC S1 Firmware version R10.3b. This could allow an adversary to access some device files.	5.8	More Details
CVE-2023-39562	GPAC v2.3-DEV-rev449-g5948e4f70-master was discovered to contain a heap-use-after-free via the gf_bs_align function at bitstream.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via supplying a crafted file.	5.5	More Details
CVE-2023-24620	An issue was discovered in Esoteric YamlBeans through 1.15. A crafted YAML document is able perform am XML Entity Expansion attack against YamlBeans YamlReader. By exploiting the Anchor feature in YAML, it is possible to generate a small YAML document that, when read, is expanded to a large size, causing CPU and memory consumption, such as a Java Out-of-Memory exception.	5.5	More Details
CVE-2023-40036	Notepad++ is a free and open-source source code editor. Versions 8.5.6 and prior are vulnerable to global buffer read overflow in `CharDistributionAnalysis::HandleOneChar`. The exploitability of this issue is not clear. Potentially, it may be used to leak internal memory allocation information. As of time of publication, no known patches are available in existing versions of Notepad++.	5.5	More Details
CVE-2023-4569	A memory leak flaw was found in nft_set_catchall_flush in net/netfilter/nf_tables_api.c in the Linux Kernel. This issue may allow a local attacker to cause double-deactivations of catchall elements, which can result in a memory leak.	5.5	More Details
CVE-2023-39742	giflib v5.2.1 was discovered to contain a segmentation fault via the component getarg.c.	5.5	More Details
CVE-2023-4508	A user able to control file input to Gerbv, between versions 2.4.0 and 2.10.0, can cause a crash and cause denial-of-service with a specially crafted Gerber RS-274X file.	5.5	More Details
CVE-2023-30436	IBM Security Guardium 11.3, 11.4, and 11.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 252292.	5.5	More Details
CVE-2023-4042	A flaw was found in ghostscript. The fix for CVE-2020-16305 in ghostscript was not included in RHSA-2021:1852-06 advisory as it was claimed to be. This issue only affects the ghostscript package as shipped with Red Hat Enterprise Linux 8.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39288	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect through 9.6.2304.102 could allow an authenticated attacker with elevated privileges and internal network access to conduct a command argument injection due to insufficient parameter sanitization. A successful exploit could allow an attacker to access network information and to generate excessive network traffic.	5.5	More Details
CVE-2023-40164	Notepad++ is a free and open-source source code editor. Versions 8.5.6 and prior are vulnerable to global buffer read overflow in `nsCodingStateMachine::NextStater`. The exploitability of this issue is not clear. Potentially, it may be used to leak internal memory allocation information. As of time of publication, no known patches are available in existing versions of Notepad++.	5.5	More Details
CVE-2023-40166	Notepad++ is a free and open-source source code editor. Versions 8.5.6 and prior are vulnerable to heap buffer read overflow in `FileManager::detectLanguageFromTextBegining `. The exploitability of this issue is not clear. Potentially, it may be used to leak internal memory allocation information. As of time of publication, no known patches are available in existing versions of Notepad++.	5.5	More Details
CVE-2023-39287	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through 19.3 SP3 (22.24.5800.0) could allow an authenticated attacker with elevated privileges and internal network access to conduct a command argument injection due to insufficient parameter sanitization. A successful exploit could allow an attacker to access network information and to generate excessive network traffic.	5.5	More Details
CVE-2023-40875	DedeCMS up to and including 5.7.110 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities at /dede/vote_edit.php via the votename and votenote parameters.	5.4	More Details
CVE-2023-38973	A stored cross-site scripting (XSS) vulnerability in the Add Tag function of Badaso v2.9.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title parameter.	5.4	More Details
CVE-2023-41153	A Stored Cross-Site Scripting (XSS) vulnerability in the SSH configuration tab in Usermin 2.001 allows remote attackers to inject arbitrary web script or HTML via options for the host value while editing the host options.	5.4	More Details
CVE-2023-38971	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 rack number parameter in the add new rack function.	5.4	More Details
CVE-2023-40282	Improper authentication vulnerability in Rakuten WiFi Pocket all versions allows a network-adjacent attacker to log in to the product's Management Screen. As a result, sensitive information may be obtained and/or the settings may be changed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4520	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_fv_player_user_video' parameter saved via the 'save' function hooked via init, and the plugin is also vulnerable to Arbitrary Usermeta Update via the 'save' function in versions up to, and including, 7.5.37.7212 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, and makes it possible to update the user metas arbitrarily, but the meta value can only be a string.	5.4	More Details
CVE-2023-40876	DedeCMS up to and including 5.7.110 was discovered to contain a cross-site scripting (XSS) vulnerability at /dede/freelist_add.php via the title parameter.	5.4	More Details
CVE-2023-20115	A vulnerability in the SFTP server implementation for Cisco Nexus 3000 Series Switches and 9000 Series Switches in standalone NX-OS mode could allow an authenticated, remote attacker to download or overwrite files from the underlying operating system of an affected device. This vulnerability is due to a logic error when verifying the user role when an SFTP connection is opened to an affected device. An attacker could exploit this vulnerability by connecting and authenticating via SFTP as a valid, non-administrator user. A successful exploit could allow the attacker to read or overwrite files from the underlying operating system with the privileges of the authenticated user. There are workarounds that address this vulnerability.	5.4	More Details
CVE-2023-40877	DedeCMS up to and including 5.7.110 was discovered to contain a cross-site scripting (XSS) vulnerability at /dede/freelist_edit.php via the title parameter.	5.4	More Details
CVE-2023-20230	A vulnerability in the restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to read, modify, or delete non-tenant policies (for example, access policies) created by users associated with a different security domain on an affected system. This vulnerability is due to improper access control when restricted security domains are used to implement multi-tenancy for policies outside the tenant boundaries. An attacker with a valid user account associated with a restricted security domain could exploit this vulnerability. A successful exploit could allow the attacker to read, modify, or delete policies created by users associated with a different security domain. Exploitation is not possible for policies under tenants that an attacker has no authorization to access.	5.4	More Details
CVE-2023-40753	There is a Cross Site Scripting (XSS) vulnerability in the message parameter of index.php in PHPJabbers Ticket Support Script v3.2.	5.4	More Details
CVE-2023-38974	A stored cross-site scripting (XSS) vulnerability in the Edit Category function of Badaso v2.9.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38969	Cross Site Scripting vulnerabiltiy in Badaso v.2.9.7 allows a remote attacker to execute arbitrary code via a crafted payload to the title parameter in the new book and edit book function.	5.4	More Details
CVE-2023-39707	A stored cross-site scripting (XSS) vulnerability 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 Add Expense parameter under the Expense section.	5.4	More Details
CVE-2023-40874	DedeCMS up to and including 5.7.110 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities at /dede/vote_add.php via the votename and voteitem1 parameters.	5.4	More Details
CVE-2023-25848	ArcGIS Enterprise Server versions 11.0 and below have an information disclosure vulnerability where a remote, unauthorized attacker may submit a crafted query that may result in a low severity information disclosure issue. The information disclosed is limited to a single attribute in a database connection string. No business data is disclosed.	5.3	More Details
CVE-2023-41100	An issue was discovered in the hcaptcha (aka hCaptcha for EXT:form) extension before 2.1.2 for TYPO3. It fails to check that the required captcha field is submitted in the form data. allowing a remote user to bypass the CAPTCHA check.	5.3	More Details
CVE-2023-32755	e-Excellence U-Office Force generates an error message in webiste service. An unauthenticated remote attacker can obtain partial sensitive system information from error message by sending a crafted command.	5.3	More Details
CVE-2023-34040	In Spring for Apache Kafka 3.0.9 and earlier and versions 2.9.10 and earlier, a possible deserialization attack vector existed, but only if unusual configuration was applied. An attacker would have to construct a malicious serialized object in one of the deserialization exception record headers. Specifically, an application is vulnerable when all of the following are true: * The user does not configure an ErrorHandlingDeserializer for the key and/or value of the record * The user explicitly sets container properties checkDeserExWhenKeyNull and/or checkDeserExWhenValueNull container properties to true. * The user allows untrusted sources to publish to a Kafka topic By default, these properties are false, and the container only attempts to deserialize the headers if an ErrorHandlingDeserializer is configured. The ErrorHandlingDeserializer prevents the vulnerability by removing any such malicious headers before processing the record.	5.3	More Details
CVE-2023-1995	Insufficient Logging vulnerability in Hitachi HiRDB Server, HiRDB Server With Addtional Function, HiRDB Structured Data Access Facility.This issue affects HiRDB Server: before 09-60-39, before 09-65-23, before 09-66-17, before 10-01-10, before 10-03-12, before 10-04-06, before 10-05-06, before 10-06-02; HiRDB Server With Addtional Function: before 09-60-2M, before 09-65-/W , before 09-66-/Q ; HiRDB Structured Data Access Facility: before 09-60-39, before 10-03-12, before 10-04-06, before 10-06-02.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4513	BT SDP dissector memory leak in Wireshark 4.0.0 to 4.0.7 and 3.6.0 to 3.6.15 allows denial of service via packet injection or crafted capture file	5.3	More Details
CVE-2023-4511	BT SDP dissector infinite loop in Wireshark 4.0.0 to 4.0.7 and 3.6.0 to 3.6.15 allows denial of service via packet injection or crafted capture file	5.3	More Details
CVE-2023-4230	A vulnerability has been identified in ioLogik 4000 Series (ioLogik E4200) firmware versions v1.6 and prior, which has the potential to facilitate the collection of information on ioLogik 4000 Series devices. This vulnerability may enable attackers to gather information for the purpose of assessing vulnerabilities and potential attack vectors.	5.3	More Details
CVE-2023-38283	In OpenBGPD before 8.1, incorrect handling of BGP update data (length of path attributes) set by a potentially distant remote actor may cause the system to incorrectly reset a session. This is fixed in OpenBSD 7.3 errata 006.	5.3	More Details
CVE-2023-3704	The vulnerability exists in CP-Plus DVR due to an improper input validation within the web-based management interface of the affected products. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable device. Successful exploitation of this vulnerability could allow the remote attacker to change system time of the targeted device.	5.3	More Details
CVE-2023-4227	A vulnerability has been identified in the ioLogik 4000 Series (ioLogik E4200) firmware versions v1.6 and prior, which can be exploited by malicious actors to potentially gain unauthorized access to the product. This could lead to security breaches, data theft, and unauthorized manipulation of sensitive information. The vulnerability is attributed to the presence of an unauthorized service, which could potentially enable unauthorized access to the. device.	5.3	More Details
CVE-2023-24548	On affected platforms running Arista EOS with VXLAN configured, malformed or truncated packets received over a VXLAN tunnel and forwarded in hardware can cause egress ports to be unable to forward packets. The device will continue to be susceptible to the issue until remediation is in place.	5.3	More Details
CVE-2023-40178	Node-SAML is a SAML library not dependent on any frameworks that runs in Node. The lack of checking of current timestamp allows a LogoutRequest XML to be reused multiple times even when the current time is past the NotOnOrAfter. This could impact the user where they would be logged out from an expired LogoutRequest. In bigger contexts, if LogoutRequests are sent out in mass to different SPs, this could impact many users on a large scale. This issue was patched in version 4.0.5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39522	goauthentik is an open-source Identity Provider. In affected versions using a recovery flow with an identification stage an attacker is able to determine if a username exists. Only setups configured with a recovery flow are impacted by this. Anyone with a user account on a system with the recovery flow described above is susceptible to having their username/email revealed as existing. An attacker can easily enumerate and check users' existence using the recovery flow, as a clear message is shown when a user doesn't exist. Depending on configuration this can either be done by username, email, or both. This issue has been addressed in versions 2023.5.6 and 2023.6.2. Users are advised to upgrade. There are no known workarounds for this issue.	5.3	More Details
CVE-2023-40612	In OpenMNS Horizon 31.0.8 and versions earlier than 32.0.2, the file editor which is accessible to any user with ROLE_FILESYSTEM_EDITOR privileges is vulnerable to XXE injection attacks. The solution is to upgrade to Meridian 2023.1.5 or Horizon 32.0.2 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Erik Wynter for reporting this issue.	5.3	More Details
CVE-2023-39559	AudimexEE 15.0 was discovered to contain a full path disclosure vulnerability.	5.3	More Details
CVE-2023-4512	CBOR dissector crash in Wireshark 4.0.0 to 4.0.6 allows denial of service via packet injection or crafted capture file	5.3	More Details
CVE-2023-1409	If the MongoDB Server running on Windows or macOS is configured to use TLS with a specific set of configuration options that are already known to work securely in other platforms (e.g. Linux), it is possible that client certificate validation may not be in effect, potentially allowing client to establish a TLS connection with the server that supplies any certificate. This issue affect all MongoDB Server v6.3 versions, MongoDB Server v5.0 versions v5.0.0 to v5.0.14 and all MongoDB Server v4.4 versions.	5.3	More Details
CVE-2023-26272	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3)) could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 248133.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40570	Datasette is an open source multi-tool for exploring and publishing data. This bug affects Datasette instances running a Datasette 1.0 alpha - 1.0a0, 1.0a1, 1.0a2 or 1.0a3 - in an online accessible location but with authentication enabled using a plugin such as datasette-auth-passwords. The `/-/api` API explorer endpoint could reveal the names of both databases and tables - but not their contents - to an unauthenticated user. Datasette 1.0a4 has a fix for this issue. This will block access to the API explorer but will still allow access to the Datasette read or write JSON APIs, as those use different URL patterns within the Datasette `/database` hierarchy. This issue is patched in version 1.0a4.	5.3	More Details
CVE-2023-30437	IBM Security Guardium 11.3, 11.4, and 11.5 could allow an unauthorized user to enumerate usernames by sending a specially crafted HTTP request. IBM X-Force ID: 252293.	5.3	More Details
CVE-2023-40179	Silverware Games is a premium social network where people can play games online. Prior to version 1.3.6, the Password Recovery form would throw an error if the specified email was not found in our database. It would only display the "Enter the code" form if the email is associated with a member of the site. Since version 1.3.6, the "Enter the code" form is always returned, showing the message "If the entered email is associated with an account, a code will be sent now". This change prevents potential violators from determining if our site has a user with the specified email.	5.3	More Details
CVE-2023-23473	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 245400.	5.3	More Details
CVE-2023-24959	IBM InfoSphere Information Systems 11.7 could expose information about the host system and environment configuration. IBM X-Force ID: 246332.	5.3	More Details
CVE-2023-26271	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3)) uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 248126.	5.3	More Details
CVE-2022-46783	An issue was discovered in Stormshield SSL VPN Client before 3.2.0. If multiple address books are used, an attacker may be able to access the other encrypted address book.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40217	An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there is a brief window where the SSLSocket instance will detect the socket as "not connected" and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.)	5.3	More Details
CVE-2023-32497	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Supersoju Block Referer Spam plugin <= 1.1.9.4 versions.	5.1	More Details
CVE-2023-39290	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect through R19.3 SP3 (22.24.5800.0) could allow an authenticated attacker with elevated privileges to conduct an information disclosure attack due to improper configuration. A successful exploit could allow an attacker to view system information.	4.9	More Details
CVE-2023-39291	A vulnerability in the Connect Mobility Router component of MiVoice Connect through 9.6.2304.102 could allow an authenticated attacker with elevated privileges to conduct an information disclosure attack due to improper configuration. A successful exploit could allow an attacker to view system information.	4.9	More Details
CVE-2020-11711	An issue was discovered in Stormshield SNS 3.8.0. Authenticated Stored XSS in the admin login panel leads to SSL VPN credential theft. A malicious disclaimer file can be uploaded from the admin panel. The resulting file is rendered on the authentication interface of the admin panel. It is possible to inject malicious HTML content in order to execute JavaScript inside a victim's browser. This results in a stored XSS on the authentication interface of the admin panel. Moreover, an unsecured authentication form is present on the authentication interface of the SSL VPN captive portal. Users are allowed to save their credentials inside the browser. If an administrator saves his credentials through this unsecured form, these credentials could be stolen via the stored XSS on the admin panel without user interaction. Another possible exploitation would be modification of the authentication form of the admin panel into a malicious form.	4.8	More Details
CVE-2023-39578	A stored cross-site scripting (XSS) vulnerability in the Create function of Zenario CMS v9.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Menu navigation text field.	4.8	More Details
CVE-2023-4561	Cross-site Scripting (XSS) - Stored in GitHub repository omeka/omeka-s prior to 4.0.4.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41167	@webiny/react-rich-text-renderer before 5.37.2 allows XSS attacks by content managers. This is a react component to render data coming from Webiny Headless CMS and Webiny Form Builder. Webiny is an open-source serverless enterprise CMS. The @webiny/react-rich-text-renderer package depends on the editor.js rich text editor to handle rich text content. The CMS stores rich text content from the editor.js into the database. When the @webiny/react-rich-text-renderer is used to render such content, it uses the dangerouslySetInnerHTML prop, without applying HTML sanitization. The issue arises when an actor, who in this context would specifically be a content manager with access to the CMS, inserts a malicious script as part of the user-defined input. This script is then injected and executed within the user's browser when the main page or admin page loads.	4.8	More Details
CVE-2023-39521	Tuleap is an open source suite to improve management of software developments and collaboration. In Tuleap Community Edition prior to version 14.11.99.28 and Tuleap Enterprise Edition prior to versions 14.10-6 and 14.11-3, content displayed in the "card fields" (visible in the kanban and PV2 apps) is not properly escaped. An agile dashboard administrator deleting a kanban with a malicious label can be forced to execute uncontrolled code. Tuleap Community Edition 14.11.99.28, Tuleap Enterprise Edition 14.10-6, and Tuleap Enterprise Edition 14.11-3 contain a fix for this issue.	4.8	More Details
CVE-2023-36317	Cross Site Scripting (XSS) vulnerability in sourcecodester Student Study Center Desk Management System 1.0 allows attackers to run arbitrary code via crafted GET request to web application URL.	4.8	More Details
CVE-2023-40025	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting from version 2.6.0 have a bug where open web terminal sessions do not expire. This bug allows users to send any websocket messages even if the token has already expired. The most straightforward scenario is when a user opens the terminal view and leaves it open for an extended period. This allows the user to view sensitive information even when they should have been logged out already. A patch for this vulnerability has been released in the following Argo CD versions: 2.6.14, 2.7.12 and 2.8.1.	4.7	More Details
CVE-2023-40530	Improper authorization in handler for custom URL scheme issue in 'Skylark' App for Android 6.2.13 and earlier and 'Skylark' App for iOS 6.2.13 and earlier allows an attacker to lead a user to access an arbitrary website via another application installed on the user's device.	4.7	More Details
CVE-2023-39801	A lack of exception handling in the Renault Easy Link Multimedia System Software Version 283C35519R allows attackers to cause a Denial of Service (DoS) via supplying crafted WMA files when connecting a device to the vehicle's USB plug and play feature.	4.6	More Details
CVE-2023-41249	In JetBrains TeamCity before 2023.05.3 reflected XSS was possible during copying Build Step	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43909	IBM Security Guardium 11.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 240905.	4.6	More Details
CVE-2023-40170	jupyter-server is the backend for Jupyter web applications. Improper cross-site credential checks on `/files/` URLs could allow exposure of certain file contents, or accessing files when opening untrusted files via "Open image in new tab". This issue has been addressed in commit `87a49272728` which has been included in release `2.7.2`. Users are advised to upgrade. Users unable to upgrade may use the lower performance `--ContentsManager.files_handler_class=jupyter_server.files.handlers.FilesHandler`, which implements the correct checks.	4.6	More Details
CVE-2023-41248	In JetBrains TeamCity before 2023.05.3 stored XSS was possible during Cloud Profiles configuration	4.6	More Details
CVE-2023-39268	A memory corruption vulnerability in ArubaOS-Switch could lead to unauthenticated remote code execution by receiving specially crafted packets. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	4.5	More Details
CVE-2022-3743	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges under certain conditions the ability to enumerate Embedded Controller (EC) commands.	4.4	More Details
CVE-2022-3745	A potential vulnerability was discovered in LCFC BIOS for some Lenovo consumer notebook models that could allow a local attacker with elevated privileges to view incoming and returned data from SMI.	4.4	More Details
CVE-2023-20234	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to create a file or overwrite any file on the filesystem of an affected device, including system files. The vulnerability occurs because there is no validation of parameters when a specific CLI command is used. An attacker could exploit this vulnerability by authenticating to an affected device and using the command at the CLI. A successful exploit could allow the attacker to overwrite any file on the disk of the affected device, including system files. The attacker must have valid administrative credentials on the affected device to exploit this vulnerability.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40587	Pyramid is an open source Python web framework. A path traversal vulnerability in Pyramid versions 2.0.0 and 2.0.1 impacts users of Python 3.11 that are using a Pyramid static view with a full filesystem path and have a `index.html` file that is located exactly one directory above the location of the static view's file system path. No further path traversal exists, and the only file that could be disclosed accidentally is `index.html`. Pyramid version 2.0.2 rejects any path that contains a null-byte out of caution. While valid in directory/file names, we would strongly consider it a mistake to use null-bytes in naming files/directories. Secondly, Python 3.11, and 3.12 has fixed the underlying issue in `os.path.normpath` to no longer truncate on the first `0x00` found, returning the behavior to pre-3.11 Python, un an as of yet unreleased version. Fixes will be available in:Python 3.12.0rc2 and 3.11.5. Some workarounds are available. Use a version of Python 3 that is not affected, downgrade to Python 3.10 series temporarily, or wait until Python 3.11.5 is released and upgrade to the latest version of Python 3.11 series.	4.3	More Details
CVE-2023-41037	OpenPGP.js is a JavaScript implementation of the OpenPGP protocol. In affected versions OpenPGP Cleartext Signed Messages are cryptographically signed messages where the signed text is readable without special tools. These messages typically contain a "Hash: ..." header declaring the hash algorithm used to compute the signature digest. OpenPGP.js up to v5.9.0 ignored any data preceding the "Hash: ..." texts when verifying the signature. As a result, malicious parties could add arbitrary text to a third-party Cleartext Signed Message, to lead the victim to believe that the arbitrary text was signed. A user or application is vulnerable to said attack vector if it verifies the CleartextMessage by only checking the returned `verified` property, discarding the associated `data` information, and instead _visually trusting_ the contents of the original message. Since `verificationResult.data` would always contain the actual signed data, users and apps that check this information are not vulnerable. Similarly, given a CleartextMessage object, retrieving the data using `getText()` or the `text` field returns only the contents that are considered when verifying the signature. Finally, re-armoring a CleartextMessage object (using `armor()` will also result in a "sanitised" version, with the extraneous text being removed. This issue has been addressed in version 5.10.1 (current stable version) which will reject messages when calling `openpgp.readCleartextMessage()` and in version 4.10.11 (legacy version) which will will reject messages when calling `openpgp.cleartext.readArmored()`. Users are advised to upgrade. Users unable to upgrade should check the contents of `verificationResult.data` to see what data was actually signed, rather than visually trusting the contents of the armored message.	4.3	More Details
CVE-2023-39968	jupyter-server is the backend for Jupyter web applications. Open Redirect Vulnerability. Maliciously crafted login links to known Jupyter Servers can cause successful login or an already logged-in session to be redirected to arbitrary sites, which should be restricted to Jupyter Server-served URLs. This issue has been addressed in commit `29036259` which is included in release 2.7.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4229	A vulnerability has been identified in ioLogik 4000 Series (ioLogik E4200) firmware versions v1.6 and prior, potentially exposing users to security risks. This vulnerability may allow attackers to trick users into interacting with malicious content, leading to unintended actions or unauthorized data disclosures.	4.3	More Details
CVE-2023-4478	Mattermost fails to restrict which parameters' values it takes from the request during signup allowing an attacker to register users as inactive, thus blocking them from later accessing Mattermost without the system admin activating their accounts.	4.3	More Details
CVE-2023-41363	In Cerebrate 1.14, a vulnerability in UserSettingsController allows authenticated users to change user settings of other users.	4.3	More Details
CVE-2023-4544	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20230809. It has been rated as problematic. This issue affects some unknown processing of the file /config/php.ini. The manipulation leads to direct request. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-238049 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-2023-3253	An improper authorization vulnerability exists where an authenticated, low privileged remote attacker could view a list of all the users available in the application.	4.3	More Details
CVE-2021-32050	Some MongoDB Drivers may erroneously publish events containing authentication-related data to a command listener configured by an application. The published events may contain security-sensitive data when specific authentication-related commands are executed. Without due care, an application may inadvertently expose this sensitive information, e.g., by writing it to a log file. This issue only arises if an application enables the command listener feature (this is not enabled by default). This issue affects the MongoDB C Driver 1.0.0 prior to 1.17.7, MongoDB PHP Driver 1.0.0 prior to 1.9.2, MongoDB Swift Driver 1.0.0 prior to 1.1.1, MongoDB Node.js Driver 3.6 prior to 3.6.10, MongoDB Node.js Driver 4.0 prior to 4.17.0 and MongoDB Node.js Driver 5.0 prior to 5.8.0. This issue also affects users of the MongoDB C++ Driver dependent on the C driver 1.0.0 prior to 1.17.7 (C++ driver prior to 3.7.0).	4.2	More Details
CVE-2023-3251	A pass-back vulnerability exists where an authenticated, remote attacker with administrator privileges could uncover stored SMTP credentials within the Nessus application.This issue affects Nessus: before 10.6.0.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39348	Spinnaker is an open source, multi-cloud continuous delivery platform. Log output when updating GitHub status is improperly set to FULL always. It's recommended to apply the patch and rotate the GitHub token used for github status notifications. Given that this would output github tokens to a log system, the risk is slightly higher than a "low" since token exposure could grant elevated access to repositories outside of control. If using READ restricted tokens, the exposure is such that the token itself could be used to access resources otherwise restricted from reads. This only affects users of GitHub Status Notifications. This issue has been addressed in pull request 1316. Users are advised to upgrade. Users unable to upgrade should disable GH Status Notifications, Filter their logs for Echo log data and use read-only tokens that are limited in scope.	4.0	More Details
CVE-2023-0238	Due to lack of a security policy, the WARP Mobile Client (<=6.29) for Android was susceptible to this vulnerability which allowed a malicious app installed on a victim's device to exploit a peculiarity in an Android function, wherein under certain conditions, the malicious app could dictate the task behaviour of the WARP app.	3.9	More Details
CVE-2023-0654	Due to a misconfiguration, the WARP Mobile Client (< 6.29) for Android was susceptible to a tapjacking attack. In the event that an attacker built a malicious application and managed to install it on a victim's device, the attacker would be able to trick the user into believing that the app shown on the screen was the WARP client when in reality it was the attacker's app.	3.9	More Details
CVE-2023-40182	Silverware Games is a premium social network where people can play games online. When using the Recovery form, a noticeably different amount of time passes depending of whether the specified email address presents in our database or not. This has been fixed in version 1.3.7.	3.7	More Details
CVE-2023-4555	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file suppliar_data.php. The manipulation of the argument name/company leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-238153 was assigned to this vulnerability.	3.5	More Details
CVE-2023-4547	A vulnerability was found in SPA-Cart eCommerce CMS 1.9.0.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /search. The manipulation of the argument filter[brandid]/filter[price] leads to cross site scripting. The attack may be launched remotely. VDB-238058 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-4546	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20230816. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /sysmanage/licence.php. The manipulation leads to improper access controls. The exploit has been disclosed to the public and may be used. The identifier VDB-238057 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-15035	A vulnerability was found in Doc2k RE-Chat 1.0. It has been classified as problematic. This affects an unknown part of the file js_on_radio-emergency.de_/re_chat.js. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The patch is named bd17d497ddd3bab4ef9c6831c747c37cc016c570. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-238155.	3.5	More Details
CVE-2023-4534	A vulnerability, which was classified as problematic, was found in NeoMind Fusion Platform up to 20230731. Affected is an unknown function of the file /fusion/portal/action/Link. The manipulation of the argument link leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-238026 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-2017-20186	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in nikooo777 ckSurf up to 1.19.2. It has been declared as problematic. This vulnerability affects the function SpecListMenuDead of the file csgo/addons/sourcemod/scripting/ckSurf/misc.sp of the component Spectator List Name Handler. The manipulation of the argument cleanName leads to denial of service. Upgrading to version 1.21.0 is able to address this issue. The name of the patch is fd6318d99083a06363091441a0614bd2f21068e6. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-238156. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2023-34972	A cleartext transmission of sensitive information vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows local network clients to read the contents of unexpected sensitive data via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QuTS hero h5.1.0.2424 build 20230609 and later	3.5	More Details
CVE-2018-25089	A vulnerability was found in glb Meetup Tag Extension 0.1 on MediaWiki. It has been rated as problematic. This issue affects some unknown processing of the component Link Attribute Handler. The manipulation leads to use of web link to untrusted target with window.opener access. Upgrading to version 0.2 is able to address this issue. The identifier of the patch is 850c726d6bbfe0bf270801fbb92a30babea4155c. It is recommended to upgrade the affected component. The identifier VDB-238157 was assigned to this vulnerability.	3.5	More Details
CVE-2023-41250	In JetBrains TeamCity before 2023.05.3 reflected XSS was possible during user registration	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4228	A vulnerability has been identified in ioLogik 4000 Series (ioLogik E4200) firmware versions v1.6 and prior, where the session cookies attribute is not set properly in the affected application. The vulnerability may lead to security risks, potentially exposing user session data to unauthorized access and manipulation.	3.1	More Details
CVE-2023-34973	An insufficient entropy vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows remote users to predict secret via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QuTS hero h5.1.0.2424 build 20230609 and later	3.1	More Details
CVE-2023-41126	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-2023-39583	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-38831. Reason: This candidate is a reservation duplicate of CVE-2023-38831. Notes: All CVE users should reference CVE-2023-38831 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-40270	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-38831. Reason: This candidate is a reservation duplicate of CVE-2023-38831. Notes: All CVE users should reference CVE-2023-38831 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-41122	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-2023-4524	Rejected reason: CVE reject in favor of CVE-2023-40547	N/A	More Details
CVE-2023-41125	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-2023-38288	Rejected reason: Not a Security Issue.	N/A	More Details
CVE-2023-38289	Rejected reason: Not a Security Issue.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40568	Rejected reason: GitHub has been informed that the requestor is working with another CNA for these vulnerabilities.	N/A	More Details
CVE-2023-41123	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-2023-41124	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details