SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 23 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-2022-36648	The hardware emulation in the of_dpa_cmd_add_l2_flood of rocker device model in QEMU, as used in 7.0.0 and earlier, allows remote attackers to crash the host qemu and potentially execute code on the host via execute a malformed program in the guest OS. Note: This has been disputed by multiple third parties as not a valid vulnerability due to the rocker device not falling within the virtualization use case.	10.0	More Details
CVE-2023-25915	Due to improper input validation, an authenticated remote attacker could execute arbitrary commands on the target system.	9.9	More Details
CVE-2023-35893	IBM Security Guardium 10.6, 11.3, 11.4, and 11.5 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 258824.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37914	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user who can view `Invitation.WebHome` can execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. This vulnerability has been patched on XWiki 14.4.8, 15.2-rc-1, and 14.10.6. Users are advised to upgrade. Users unable to upgrade may manually apply the patch on `Invitation.InvitationCommon` and `Invitation.InvitationConfig`, but there are otherwise no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-39660	An issue in Gaberiele Venturi pandasai v.0.8.0 and before allows a remote attacker to execute arbitrary code via a crafted request to the prompt function.	9.8	More Details
CVE-2023-39618	TOTOLINK X5000R B20210419 was discovered to contain a remote code execution (RCE) vulnerability via the setTracerouteCfg interface.	9.8	More Details
CVE-2023-39747	TP-Link WR841N V8, TP-Link TL-WR940N V2, and TL-WR941ND V5 were discovered to contain a buffer overflow via the radiusSecret parameter at /userRpm/WlanSecurityRpm.	9.8	More Details
CVE-2023-39749	D-Link DAP-2660 v1.13 was discovered to contain a buffer overflow via the component /adv_resource. This vulnerability is exploited via a crafted GET request.	9.8	More Details
CVE-2023-39750	D-Link DAP-2660 v1.13 was discovered to contain a buffer overflow via the f_ipv6_enable parameter at /bsc_ipv6. This vulnerability is exploited via a crafted POST request.	9.8	More Details
CVE-2023-39751	TP-Link TL-WR941ND V6 were discovered to contain a buffer overflow via the pSize parameter at /userRpm/PingIframeRpm.	9.8	More Details
CVE-2020-28715	An issue was discovered in kdmserver service in LeEco LeTV X43 version V2401RCN02C080080B04121S, allows attackers to execute arbitrary code, escalate privileges, and cause a denial of service (DoS).	9.8	More Details
CVE-2023-31447	user_login.cgi on Draytek Vigor2620 devices before 3.9.8.4 (and on all versions of Vigor2925 devices) allows attackers to send a crafted payload to modify the content of the code segment, insert shellcode, and execute arbitrary code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32002	The use of `Module._load()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.	9.8	More Details
CVE-2023-38035	A security vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry versions 9.18.0 and below, which may allow an attacker to bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration.	9.8	More Details
CVE-2023-38961	Buffer Overflwo vulnerability in JerryScript Project jerryscript v.3.0.0 allows a remote attacker to execute arbitrary code via the scanner_is_context_needed component in js-scanner-until.c.	9.8	More Details
CVE-2020-26037	Directory Traversal vulnerability in Server functionalty in Even Balance Punkbuster version 1.902 before 1.905 allows remote attackers to execute arbitrary code.	9.8	More Details
CVE-2023-4373	Inadequate validation of permissions when employing remote tools and macros within Devolutions Remote Desktop Manager versions 2023.2.19 and earlier permits a user to initiate a connection without proper execution rights via the remote tools feature.	9.8	More Details
CVE-2023-39809	N.V.K.INTER CO., LTD. (NVK) iBSG v3.5 was discovered to contain a command injection vulnerability via the system_hostname parameter at /manage/network-basic.php.	9.8	More Details
CVE-2021-32292	An issue was discovered in json-c from 20200420 (post 0.14 unreleased code) through 0.15-20200726. A stack-buffer-overflow exists in the auxiliary sample program json_parse which is located in the function parseit.	9.8	More Details
CVE-2021-33388	dpic 2021.04.10 has a Heap Buffer Overflow in themakevar() function in dpic.y	9.8	More Details
CVE-2021-33390	dpic 2021.04.10 has a use-after-free in thedeletestringbox() function in dpic.y. A different vulnerablility than CVE-2021-32421.	9.8	More Details
CVE-2022-45611	An issue was discovered in Fresenius Kabi PharmaHelp 5.1.759.0 allows attackers to gain escalated privileges via via capture of user login information.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48174	There is a stack overflow vulnerability in ash.c:6030 in busybox before 1.35. In the environment of Internet of Vehicles, this vulnerability can be executed from command to arbitrary code execution.	9.8	More Details
CVE-2022-48522	In Perl 5.34.0, function S_find_uninit_var in sv.c has a stack-based crash that can lead to remote code execution or local privilege escalation.	9.8	More Details
CVE-2022-48565	An XML External Entity (XXE) issue was discovered in Python through 3.9.1. The plistlib module no longer accepts entity declarations in XML plist files to avoid XML vulnerabilities.	9.8	More Details
CVE-2023-36281	An issue in langchain v.0.0.171 allows a remote attacker to execute arbitrary code via a JSON file to load_prompt. This is related to __subclasses__ or a template.	9.8	More Details
CVE-2023-39617	TOTOLINK X5000R_V9.1.0cu.2089_B20211224 and X5000R_V9.1.0cu.2350_B20230313 were discovered to contain a remote code execution (RCE) vulnerability via the lang parameter in the setLanguageCfg function.	9.8	More Details
CVE-2023-39808	N.V.K.INTER CO., LTD. (NVK) iBSG v3.5 was discovered to contain a hardcoded root password which allows attackers to login with root privileges via the SSH service.	9.8	More Details
CVE-2023-33663	In the module “Customization fields fee for your store” (aicustomfee) from ai-dev module for PrestaShop, an attacker can perform SQL injection up to 0.2.0. Release 0.2.1 fixed this security issue.	9.8	More Details
CVE-2023-39807	N.V.K.INTER CO., LTD. (NVK) iBSG v3.5 was discovered to contain a SQL injection vulnerability via the a_passwd parameter at /portal/user-register.php.	9.8	More Details
CVE-2023-39115	install/aiz-uploader/upload in Campcodes Online Matrimonial Website System Script 3.3 allows XSS via a crafted SVG document.	9.8	More Details
CVE-2023-38894	A Prototype Pollution issue in Cronvel Tree-kit v.0.7.4 and before allows a remote attacker to execute arbitrary code via the extend function.	9.8	More Details
CVE-2023-39846	An issue in Konga v0.14.9 allows attackers to bypass authentication via a crafted JWT token.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2917	The Rockwell Automation Thinmanager Thinserver is impacted by an improper input validation vulnerability. Due to an improper input validation, a path traversal vulnerability exists, via the filename field, when the ThinManager processes a certain function. If exploited, an unauthenticated remote attacker can upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. A malicious user could exploit this vulnerability by sending a crafted synchronization protocol message and potentially gain remote code execution abilities.	9.8	More Details
CVE-2023-26469	In Jorani 1.0.0, an attacker could leverage path traversal to access files and execute code on the server.	9.8	More Details
CVE-2023-36845	A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series and SRX Series allows an unauthenticated, network-based attacker to remotely execute code. Using a crafted request which sets the variable PHPRC an attacker is able to modify the PHP execution environment allowing the injection und execution of code. This issue affects Juniper Networks Junos OS on EX Series and SRX Series: * All versions prior to 20.4R3-S9; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S7; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; * 22.4 versions prior to 22.4R2-S1, 22.4R3; * 23.2 versions prior to 23.2R1-S1, 23.2R2.	9.8	More Details
CVE-2023-39970	Unrestricted Upload of File with Dangerous Type vulnerability in AcyMailing component for Joomla. It allows remote code execution.	9.8	More Details
CVE-2023-39665	D-Link DIR-868L fw_revA_1-12_eu_multi_20170316 was discovered to contain a buffer overflow via the acStack_50 parameter.	9.8	More Details
CVE-2023-39666	D-Link DIR-842 fw_revA_1-02_eu_multi_20151008 was discovered to contain multiple buffer overflows in the fgets function via the acStack_120 and acStack_220 parameters.	9.8	More Details
CVE-2023-39667	D-Link DIR-868L fw_revA_1-12_eu_multi_20170316 was discovered to contain a buffer overflow via the param_2 parameter in the FUN_0000acb4 function.	9.8	More Details
CVE-2023-39668	D-Link DIR-868L fw_revA_1-12_eu_multi_20170316 was discovered to contain a buffer overflow via the param_2 parameter in the inet_ntoa() function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39670	Tenda AC6 _US_AC6V1.0BR_V15.03.05.16 was discovered to contain a buffer overflow via the function fgets.	9.8	More Details
CVE-2023-39671	D-Link DIR-880 A1_FW107WWb08 was discovered to contain a buffer overflow via the function FUN_0001be68.	9.8	More Details
CVE-2023-39672	Tenda WH450 v1.0.0.18 was discovered to contain a buffer overflow via the function fgets.	9.8	More Details
CVE-2023-39673	Tenda AC15 V1.0BR_V15.03.05.18_multi_TD01 was discovered to contain a buffer overflow via the function FUN_00010e34().	9.8	More Details
CVE-2023-39674	D-Link DIR-880 A1_FW107WWb08 was discovered to contain a buffer overflow via the function fgets.	9.8	More Details
CVE-2023-32626	Hidden functionality vulnerability in LAN-W300N/RS all versions, and LAN-W300N/PR5 all versions allows an unauthenticated attacker to log in to the product's certain management console and execute arbitrary OS commands.	9.8	More Details
CVE-2023-35991	Hidden functionality vulnerability in LOGITEC wireless LAN routers allows an unauthenticated attacker to log in to the product's certain management console and execute arbitrary OS commands. Affected products and versions are as follows: LAN-W300N/DR all versions, LAN-WH300N/DR all versions, LAN-W300N/P all versions, LAN-WH450N/GP all versions, LAN-WH300AN/DGP all versions, LAN-WH300N/DGP all versions, and LAN-WH300ANDGPE all versions.	9.8	More Details
CVE-2023-39454	Buffer overflow vulnerability in WRC-X1800GS-B v1.13 and earlier, WRC-X1800GSA-B v1.13 and earlier, and WRC-X1800GSH-B v1.13 and earlier allows an unauthenticated attacker to execute arbitrary code.	9.8	More Details
CVE-2023-40069	OS command injection vulnerability in ELECOM wireless LAN routers allows an attacker who can access the product to execute an arbitrary OS command by sending a specially crafted request. Affected products and versions are as follows: WRC-F1167ACF all versions, WRC-1750GHBK all versions, WRC-1167GHBK2 all versions, WRC-1750GHBK2-I all versions, and WRC-1750GHBK-E all versions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24989	TerraMaster NAS through 4.2.30 allows remote WAN attackers to execute arbitrary code as root via the raidtype and diskstring parameters for PHP Object Instantiation to the api.php?mobile/createRaid URI. (Shell metacharacters can be placed in raidtype because popen is used without any sanitization.) The credentials from CVE-2022-24990 exploitation can be used.	9.8	More Details
CVE-2023-40171	Dispatch is an open source security incident management tool. The server response includes the JWT Secret Key used for signing JWT tokens in error message when the `Dispatch Plugin - Basic Authentication Provider` plugin encounters an error when attempting to decode a JWT token. Any Dispatch users who own their instance and rely on the `Dispatch Plugin - Basic Authentication Provider` plugin for authentication may be impacted, allowing for any account to be taken over within their own instance. This could be done by using the secret to sign attacker crafted JWTs. If you think that you may be impacted, we strongly suggest you to rotate the secret stored in the `DISPATCH_JWT_SECRET` envvar in the `.env` file. This issue has been addressed in commit `b1942a4319` which has been included in the `20230817` release. users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2023-39939	SQL injection vulnerability in LuxCal Web Calendar prior to 5.2.3M (MySQL version) and LuxCal Web Calendar prior to 5.2.3L (SQLite version) allows a remote unauthenticated attacker to execute arbitrary queries against the database and obtain or alter the information in it.	9.1	More Details
CVE-2020-24113	Directory Traversal vulnerability in Contacts File Upload Interface in Yealink W60B version 77.83.0.85, allows attackers to gain sensitive information and cause a denial of service (DoS).	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-38890	Online Shopping Portal Project 3.1 allows remote attackers to execute arbitrary SQL commands/queries via the login form, leading to unauthorized access and potential data manipulation. This vulnerability arises due to insufficient validation of user-supplied input in the username field, enabling SQL Injection attacks.	8.8	More Details
CVE-2023-39944	OS command injection vulnerability in WRC-F1167ACF all versions, and WRC-1750GHBK all versions allows an attacker who can access the product to execute an arbitrary OS command by sending a specially crafted request.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1977	The Booking Manager WordPress plugin before 2.0.29 does not validate URLs input in it's admin panel or in shortcodes for showing events from a remote .ics file, allowing an attacker with privileges as low as Subscriber to perform SSRF attacks on the sites internal network.	8.8	More Details
CVE-2023-40341	A cross-site request forgery (CSRF) vulnerability in Jenkins Blue Ocean Plugin 1.27.5 and earlier allows attackers to connect to an attacker-specified URL, capturing GitHub credentials associated with an attacker-specified job.	8.8	More Details
CVE-2023-2910	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in Printer service functionality in ASUSTOR Data Master (ADM) allows remote unauthorized users to execute arbitrary commands via unspecified vectors. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.	8.8	More Details
CVE-2023-39445	Hidden functionality vulnerability in LAN-WH300N/RE all versions provided by LOGITEC CORPORATION allows an unauthenticated attacker to execute arbitrary code by sending a specially crafted file to the product's certain management console.	8.8	More Details
CVE-2023-39455	OS command injection vulnerability in ELECOM wireless LAN routers allows an authenticated user to execute an arbitrary OS command by sending a specially crafted request. Affected products and versions are as follows: WRC-600GHBK-A all versions, WRC-1467GHBK-A all versions, WRC-1900GHBK-A all versions, WRC-733FEBK2-A all versions, WRC-F1167ACF2 all versions, WRC-1467GHBK-S all versions, and WRC-1900GHBK-S all versions.	8.8	More Details
CVE-2023-39106	An issue in Nacos Group Nacos Spring Project v.1.1.1 and before allows a remote attacker to execute arbitrary code via the SnakeYamls Constructor() component.	8.8	More Details
CVE-2023-40072	OS command injection vulnerability in ELECOM wireless LAN access point devices allows an authenticated user to execute an arbitrary OS command by sending a specially crafted request.	8.8	More Details
CVE-2020-25887	Buffer overflow in mg_resolve_from_hosts_file in Mongoose 6.18, when reading from a crafted hosts file.	8.8	More Details
CVE-2023-40336	A cross-site request forgery (CSRF) vulnerability in Jenkins Folders Plugin 6.846.v23698686f0f6 and earlier allows attackers to copy folders.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38836	File Upload vulnerability in BoidCMS v.2.0.0 allows a remote attacker to execute arbitrary code by adding a GIF header to bypass MIME type checks.	8.8	More Details
CVE-2023-39975	kdc/do_tgs_req.c in MIT Kerberos 5 (aka krb5) 1.21 before 1.21.2 has a double free that is reachable if an authenticated user can trigger an authorization-data handling failure. Incorrect data is copied from one ticket to another.	8.8	More Details
CVE-2020-24292	Buffer Overflow vulnerability in load function in PluginICO.cpp in FreeImage 3.19.0 [r1859] allows remote attackers to run arbitrary code via opening of crafted ico file.	8.8	More Details
CVE-2023-34213	TN-5900 Series firmware versions v3.3 and prior are vulnerable to command-injection vulnerability. This vulnerability stems from insufficient input validation and improper authentication in the key-generation function, which could potentially allow malicious users to execute remote code on affected devices.	8.8	More Details
CVE-2023-33239	TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command injection vulnerability. This vulnerability stems from insufficient input validation in the key-generation function, which could potentially allow malicious users to execute remote code on affected devices.	8.8	More Details
CVE-2020-24295	Buffer Overflow vulnerability in PSDParser.cpp::ReadImageLine() in FreeImage 3.19.0 [r1859] allows remote attackers to ru narbitrary code via use of crafted psd file.	8.8	More Details
CVE-2023-33237	TN-5900 Series firmware version v3.3 and prior is vulnerable to improper-authentication vulnerability. This vulnerability arises from inadequate authentication measures implemented in the web API handler, allowing low-privileged APIs to execute restricted actions that only high-privileged APIs are allowed This presents a potential risk of unauthorized exploitation by malicious actors.	8.8	More Details
CVE-2023-0579	The YARPP WordPress plugin before 5.30.3 does not validate and escape some of its shortcode attributes before using them in SQL statement/s, which could allow any authenticated users, such as subscribers to perform SQL Injection attacks.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38902	A command injection vulnerability in RG-EW series home routers and repeaters v.EW_3.0(1)B11P219, RG-NBS and RG-S1930 series switches v.SWITCH_3.0(1)B11P219, RG-EG series business VPN routers v.EG_3.0(1)B11P219, EAP and RAP series wireless access points v.AP_3.0(1)B11P219, and NBC series wireless controllers v.AC_3.0(1)B11P219 allows an authorized attacker to execute arbitrary commands on remote devices by sending a POST request to /cgi-bin/luci/api/cmd via the remoteIp field.	8.8	More Details
CVE-2023-38132	LAN-W451NGR all versions provided by LOGITEC CORPORATION contains an improper access control vulnerability, which allows an unauthenticated attacker to log in to telnet service.	8.8	More Details
CVE-2021-40263	A heap overflow vulnerability in FreeImage 1.18.0 via the ofLoad function in PluginTIFF.cpp.	8.8	More Details
CVE-2023-36787	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.8	More Details
CVE-2020-19726	An issue was discovered in binutils libbfd.c 2.36 relating to the auxiliary symbol data allows attackers to read or write to system memory or cause a denial of service.	8.8	More Details
CVE-2020-24293	Buffer Overflow vulnerability in psdThumbnail::Read in PSDParser.cpp in FreeImage 3.19.0 [r1859] allows remote attackers to run arbitrary code via opening of crafted psd file.	8.8	More Details
CVE-2023-23564	An issue was discovered in Geomatika IsiGeo Web 6.0. It allows remote authenticated users to execute commands.	8.8	More Details
CVE-2023-25914	Due to improper restriction, authenticated attackers could retrieve and read system files of the underlying server through the XML interface. The information that can be read can lead to a full system compromise.	8.8	More Details
CVE-2022-26592	Stack Overflow vulnerability in libsass 3.6.5 via the CompoundSelector::has_real_parent_ref function.	8.8	More Details
CVE-2020-18232	Buffer Overflow vulnerability in function H5S_close in H5S.c in HDF5 1.10.4 allows remote attackers to run arbitrary code via creation of crafted file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18494	Buffer Overflow vulnerability in function H5S_close in H5S.c in HDF5 1.10.4 allows remote attackers to run arbitrary code via creation of crafted file.	8.8	More Details
CVE-2021-40265	A heap overflow bug exists FreeImage before 1.18.0 via ofLoad function in PluginJPEG.cpp.	8.8	More Details
CVE-2023-3699	An Improper Privilege Management vulnerability was found in ASUSTOR Data Master (ADM) allows an unprivileged local users to modify the storage devices configuration. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.	8.7	More Details
CVE-2023-2318	DOM-based XSS in src/muya/lib/contentState/pasteCtrl.js in MarkText 0.17.1 and before on Windows, Linux and macOS allows arbitrary JavaScript code to run in the context of MarkText main window. This vulnerability can be exploited if a user copies text from a malicious webpage and paste it into MarkText.	8.6	More Details
CVE-2023-2317	DOM-based XSS in updater/update.html in Typora before 1.6.7 on Windows and Linux allows a crafted markdown file to run arbitrary JavaScript code in the context of Typora main window via loading typora://app/typemark/updater/update.html in <embed> tag. This vulnerability can be exploited if a user opens a malicious markdown file in Typora, or copies text from a malicious webpage and paste it into Typora.	8.6	More Details
CVE-2020-23793	An issue was discovered in spice-server spice-server-0.14.0-6.el7_6.1.x86_64 of Redhat's VDI product. There is a security vulnerablility that can restart KVMvirtual machine without any authorization. It is not yet known if there will be other other effects.	8.6	More Details
CVE-2023-3698	Printer service fails to adequately handle user input, allowing an remote unauthorized users to navigate beyond the intended directory structure and delete files. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.	8.5	More Details
CVE-2023-3958	The WP Remote Users Sync plugin for WordPress is vulnerable to Server Side Request Forgery via the 'notify_ping_remote' AJAX function in versions up to, and including, 1.2.12. This can allow authenticated attackers with subscriber-level permissions or above to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. This was partially patched in version 1.2.12 and fully patched in version 1.2.13.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3697	Printer service fails to adequately handle user input, allowing an remote unauthorized users to navigate beyond the intended directory structure and create files. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.	8.5	More Details
CVE-2023-4030	A vulnerability was reported in BIOS for ThinkPad P14s Gen 2, P15s Gen 2, T14 Gen 2, and T15 Gen 2 that could cause the system to recover to insecure settings if the BIOS becomes corrupt.	8.4	More Details
CVE-2022-46751	Improper Restriction of XML External Entity Reference, XML Injection (aka Blind XPath Injection) vulnerability in Apache Software Foundation Apache Ivy.This issue affects any version of Apache Ivy prior to 2.5.2. When Apache Ivy prior to 2.5.2 parses XML files - either its own configuration, Ivy files or Apache Maven POMs - it will allow downloading external document type definitions and expand any entity references contained therein when used. This can be used to exfiltrate data, access resources only the machine running Ivy has access to or disturb the execution of Ivy in different ways. Starting with Ivy 2.5.2 DTD processing is disabled by default except when parsing Maven POMs where the default is to allow DTD processing but only to include a DTD snippet shipping with Ivy that is needed to deal with existing Maven POMs that are not valid XML files but are nevertheless accepted by Maven. Access can be be made more lenient via newly introduced system properties where needed. Users of Ivy prior to version 2.5.2 can use Java system properties to restrict processing of external DTDs, see the section about "JAXP Properties for External Access restrictions" inside Oracle's "Java API for XML Processing (JAXP) Security Guide".	8.2	More Details
CVE-2023-2110	Improper path handling in Obsidian desktop before 1.2.8 on Windows, Linux and macOS allows a crafted webpage to access local files and exfiltrate them to remote web servers via "app://local/<absolute-path>". This vulnerability can be exploited if a user opens a malicious markdown file in Obsidian, or copies text from a malicious webpage and paste it into Obsidian.	8.2	More Details
CVE-2023-37424	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host if certain preconditions outside of the attacker's control are met. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37421	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	8.1	More Details
CVE-2023-37422	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	8.1	More Details
CVE-2023-37423	Vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	8.1	More Details
CVE-2023-40034	Woodpecker is a community fork of the Drone CI system. In affected versions an attacker can post malformed webhook data witch lead to an update of the repository data that can e.g. allow the takeover of an repo. This is only critical if the CI is configured for public usage and connected to a forge witch is also in public usage. This issue has been addressed in version 1.0.2. Users are advised to upgrade. Users unable to upgrade should secure the CI system by making it inaccessible to untrusted entities, for example, by placing it behind a firewall.	8.1	More Details
CVE-2023-20211	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by authenticating to the application as a user with read-only or higher privileges and sending crafted HTTP requests to an affected system. A successful exploit could allow the attacker to read or modify data in the underlying database or elevate their privileges.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34217	TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability stems from insufficient input validation in the certificate-delete function, which could potentially allow malicious users to delete arbitrary files.	8.1	More Details
CVE-2023-34216	TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability derives from insufficient input validation in the key-delete function, which could potentially allow malicious users to delete arbitrary files.	8.1	More Details
CVE-2023-37425	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	8.0	More Details
CVE-2023-38576	Hidden functionality vulnerability in LAN-WH300N/RE all versions provided by LOGITEC CORPORATION allows an authenticated user to execute arbitrary OS commands on a certain management console.	8.0	More Details
CVE-2023-38843	An issue in Atlos v.1.0 allows an authenticated attacker to execute arbitrary code via a crafted payload into the description field in the incident function.	8.0	More Details
CVE-2022-47695	An issue was discovered Binutils objdump before 2.39.3 allows attackers to cause a denial of service or other unspecified impacts via function bfd_mach_o_get_synthetic_symtab in match-o.c.	7.8	More Details
CVE-2023-20224	A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient input validation of user-supplied CLI arguments. An attacker could exploit this vulnerability by authenticating to an affected device and using crafted commands at the prompt. A successful exploit could allow the attacker to execute arbitrary commands as root. The attacker must have valid credentials on the affected device.	7.8	More Details
CVE-2022-47673	An issue was discovered in Binutils addr2line before 2.39.3, function parse_module contains multiple out of bound reads which may cause a denial of service or other unspecified impacts.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47069	p7zip 16.02 was discovered to contain a heap-buffer-overflow vulnerability via the function NArchive::NZip::CInArchive::FindCd(bool) at CPP/7zip/Archive/Zip/ZipIn.cpp.	7.8	More Details
CVE-2022-47696	An issue was discovered Binutils objdump before 2.39.3 allows attackers to cause a denial of service or other unspecified impacts via function compare_symbols.	7.8	More Details
CVE-2023-3078	An uncontrolled search path vulnerability was reported in the Lenovo Universal Device Client (UDC) that could allow an attacker with local access to execute code with elevated privileges.	7.8	More Details
CVE-2022-45703	Heap buffer overflow vulnerability in binutils readelf before 2.40 via function display_debug_section in file readelf.c.	7.8	More Details
CVE-2023-4383	A vulnerability, which was classified as critical, was found in MicroWorld eScan Anti-Virus 7.0.32 on Linux. This affects an unknown part of the file runasroot. The manipulation leads to incorrect execution-assigned permissions. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-237315. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2022-44840	Heap buffer overflow vulnerability in binutils readelf before 2.40 via function find_section_in_set in file readelf.c.	7.8	More Details
CVE-2020-18831	Buffer Overflow vulnerability in tEXtToDataBuf function in pngimage.cpp in Exiv2 0.27.1 allows remote attackers to cause a denial of service and other unspecified impacts via use of crafted file.	7.8	More Details
CVE-2023-32495	Dell PowerScale OneFS, 8.2.x-9.5.x, contains a exposure of sensitive information to an unauthorized Actor vulnerability. An authorized local attacker could potentially exploit this vulnerability, leading to escalation of privileges.	7.8	More Details
CVE-2020-22219	Buffer Overflow vulnerability in function bitwriter_grow_ in flac before 1.4.0 allows remote attackers to run arbitrary code via crafted input to the encoder.	7.8	More Details
CVE-2020-21427	Buffer Overflow vulnerability in function LoadPixelDataRLE8 in PluginBMP.cpp in FreeImage 3.18.0 allows remote attackers to run arbitrary code and cause other impacts via crafted image file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38899	SQL injection vulnerability in berkaygediz O_Blog v.1.0 allows a local attacker to escalate privileges via the secure_file_priv component.	7.8	More Details
CVE-2020-21428	Buffer Overflow vulnerability in function LoadRGB in PluginDDS.cpp in FreeImage 3.18.0 allows remote attackers to run arbitrary code and cause other impacts via crafted image file.	7.8	More Details
CVE-2020-21890	Buffer Overflow vulnerability in clj_media_size function in devices/gdevclj.c in Artifex Ghostscript 9.50 allows remote attackers to cause a denial of service or other unspecified impact(s) via opening of crafted PDF document.	7.8	More Details
CVE-2023-34853	Buffer Overflow vulnerability in Supermicro motherboard X12DPG-QR 1.4b allows local attackers to hijack control flow via manipulation of SmcSecurityEraseSetupVar variable.	7.8	More Details
CVE-2020-21722	Buffer Overflow vulnerability in oggvideotools 0.9.1 allows remote attackers to run arbitrary code via opening of crafted ogg file.	7.8	More Details
CVE-2020-19725	There is a use-after-free vulnerability in file pdd_simplifier.cpp in Z3 before 4.8.8. It occurs when the solver attempt to simplify the constraints and causes unexpected memory access. It can cause segmentation faults or arbitrary code execution.	7.8	More Details
CVE-2023-39250	Dell Storage Integration Tools for VMware (DSITV) and Dell Storage vSphere Client Plugin (DSVCP) versions prior to 6.1.1 and Replay Manager for VMware (RMSV) versions prior to 3.1.2 contain an information disclosure vulnerability. A local low-privileged malicious user could potentially exploit this vulnerability to retrieve an encryption key that could aid in further attacks.	7.8	More Details
CVE-2023-32487	Dell PowerScale OneFS, 8.2.x - 9.5.0.x, contains an elevation of privilege vulnerability. A low privileged local attacker could potentially exploit this vulnerability, leading to denial of service, code execution and information disclosure.	7.8	More Details
CVE-2020-21724	Buffer Overflow vulnerability in ExtractorInformation function in streamExtractor.cpp in oggvideotools 0.9.1 allows remaote attackers to run arbitrary code via opening of crafted ogg file.	7.8	More Details
CVE-2020-21426	Buffer Overflow vulnerability in function C_IStream::read in PluginEXR.cpp in FreeImage 3.18.0 allows remote attackers to run arbitrary code and cause other impacts via crafted image file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39415	Improper authentication vulnerability in Proself Enterprise/Standard Edition Ver5.61 and earlier, Proself Gateway Edition Ver1.62 and earlier, and Proself Mail Sanitize Edition Ver1.07 and earlier allow a remote unauthenticated attacker to log in to the product's Control Panel and perform an unintended operation.	7.5	More Details
CVE-2022-28070	A null pointer deference in __core_anal_fcn function in radare2 5.4.2 and 5.4.0.	7.5	More Details
CVE-2023-38838	SQL injection vulnerability in Kidus Minimati v.1.0.0 allows a remote attacker to obtain sensitive information via the edit.php component.	7.5	More Details
CVE-2023-39141	webui-aria2 commit 4fe2e was discovered to contain a path traversal vulnerability.	7.5	More Details
CVE-2023-37369	In Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.2, there can be an application crash in QXmlStreamReader via a crafted XML string that triggers a situation in which a prefix is greater than a length.	7.5	More Details
CVE-2020-20813	Control Channel in OpenVPN 2.4.7 and earlier allows remote attackers to cause a denial of service via crafted reset packet.	7.5	More Details
CVE-2020-21699	The web server Tengine 2.2.2 developed in the Nginx version from 0.5.6 thru 1.13.2 is vulnerable to an integer overflow vulnerability in the nginx range filter module, resulting in the leakage of potentially sensitive information triggered by specially crafted requests.	7.5	More Details
CVE-2022-28071	A use after free in r_reg_get_name_idx function in radare2 5.4.2 and 5.4.0.	7.5	More Details
CVE-2022-28072	A heap buffer overflow in r_read_le32 function in radare25.4.2 and 5.4.0.	7.5	More Details
CVE-2022-28073	A use after free in r_reg_set_value function in radare2 5.4.2 and 5.4.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3604	The Change WP Admin Login WordPress plugin before 1.1.4 discloses the URL of the hidden login page when accessing a crafted URL, bypassing the protection offered.	7.5	More Details
CVE-2023-40272	Apache Airflow Spark Provider, versions before 4.1.3, is affected by a vulnerability that allows an attacker to pass in malicious parameters when establishing a connection giving an opportunity to read files on the Airflow server. It is recommended to upgrade to a version that is not affected.	7.5	More Details
CVE-2022-28069	A heap buffer overflow in vax_opfunction in radare2 5.4.2 and 5.4.0.	7.5	More Details
CVE-2021-34193	Stack overflow vulnerability in OpenSC smart card middleware before 0.23 via crafted responses to APDUs.	7.5	More Details
CVE-2023-36106	An incorrect access control vulnerability in powerjob 4.3.2 and earlier allows remote attackers to obtain sensitive information via the interface for querying via appId parameter to /container/list.	7.5	More Details
CVE-2021-46174	Heap-based Buffer Overflow in function bfd_getl32 in Binutils objdump 3.37.	7.5	More Details
CVE-2023-39026	Directory Traversal vulnerability in FileMage Gateway Windows Deployments v.1.10.8 and before allows a remote attacker to obtain sensitive information via a crafted request to the /mgmt/ component.	7.5	More Details
CVE-2022-25024	The json2xml package through 3.12.0 for Python allows an error in typecode decoding enabling a remote attack that can lead to an exception, causing a denial of service.	7.5	More Details
CVE-2023-25913	Because of an authentication flaw an attacker would be capable of generating a web report that discloses sensitive information such as internal IP addresses, usernames, store names and other sensitive information.	7.5	More Details
CVE-2023-33850	IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information.	7.5	More Details
CVE-2023-4241	lol-html can cause panics on certain HTML inputs. Anyone processing arbitrary 3rd party HTML with the library is affected.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40211	An issue was discovered with ImageMagick 7.1.0-4 via Division by zero in function ReadEnhMetaFile of coders/emf.c.	7.5	More Details
CVE-2023-4475	An Arbitrary File Movement vulnerability was found in ASUSTOR Data Master (ADM) allows an attacker to exploit the file renaming feature to move files to unintended directories. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.	7.5	More Details
CVE-2023-39125	NTSC-CRT 2.2.1 has an integer overflow and out-of-bounds write in loadBMP in bmp_rw.c because a file's width, height, and BPP are not validated. NOTE: the vendor's perspective is "this main application was not intended to be a well tested program, it's just something to demonstrate it works and for the user to see how to integrate it into their own programs."	7.5	More Details
CVE-2023-2915	The Rockwell Automation Thinmanager Thinserver is impacted by an improper input validation vulnerability, Due to improper input validation, a path traversal vulnerability exists when the ThinManager software processes a certain function. If exploited, an unauthenticated remote threat actor can delete arbitrary files with system privileges. A malicious user could exploit this vulnerability by sending a specifically crafted synchronization protocol message resulting in a denial-of-service condition.	7.5	More Details
CVE-2023-2914	The Rockwell Automation Thinmanager Thinserver is impacted by an improper input validation vulnerability, an integer overflow condition exists in the affected products. When the ThinManager processes incoming messages, a read access violation occurs and terminates the process. A malicious user could exploit this vulnerability by sending a crafted synchronization protocol message and causing a denial of service condition in the software.	7.5	More Details
CVE-2023-39669	D-Link DIR-880 A1_FW107WWb08 was discovered to contain a NULL pointer dereference in the function FUN_00010824.	7.5	More Details
CVE-2021-35309	An issue discovered in Samsung SyncThru Web Service SPL 5.93 06-09-2014 allows attackers to gain escalated privileges via MITM attacks.	7.5	More Details
CVE-2022-28068	A heap buffer overflow in r_sleb128 function in radare2 5.4.2 and 5.4.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34038	Etcd v3.5.4 allows remote attackers to cause a denial of service via function PageWriter.write in pagewriter.go. NOTE: the vendor's position is that this is not a vulnerability.	7.5	More Details
CVE-2021-32422	dpic 2021.01.01 has a Global buffer overflow in theyylex() function in main.c and reads out of the bound array.	7.5	More Details
CVE-2022-48570	Crypto++ through 8.4 contains a timing side channel in ECDSA signature generation. Function FixedSizeAllocatorWithCleanup could write to memory outside of the allocation if the allocated memory was not 16-byte aligned. NOTE: this issue exists because the CVE-2019-14318 fix was intentionally removed for functionality reasons.	7.5	More Details
CVE-2023-38839	SQL injection vulnerability in Kidus Minimati v.1.0.0 allows a remote attacker to obtain sensitive information via theID parameter in the fulldelete.php component.	7.5	More Details
CVE-2020-23804	Uncontrolled Recursion in pdfinfo, and pdftops in poppler 0.89.0 allows remote attackers to cause a denial of service via crafted input.	7.5	More Details
CVE-2022-48571	memcached 1.6.7 allows a Denial of Service via multi-packet uploads in UDP.	7.5	More Details
CVE-2022-48560	A use-after-free exists in Python through 3.9 via heappushpop in heapq.	7.5	More Details
CVE-2023-40711	Veilid before 0.1.9 does not check the size of uncompressed data during decompression upon an envelope receipt, which allows remote attackers to cause a denial of service (out-of-memory abort) via crafted packet data, as exploited in the wild in August 2023.	7.5	More Details
CVE-2023-39784	Tenda AC8V4 V16.03.34.06 was discovered to contain a stack overflow via the list parameter in the save_virtualser_data function.	7.5	More Details
CVE-2023-39785	Tenda AC8V4 V16.03.34.06 was discovered to contain a stack overflow via the list parameter in the set_qosMib_list function.	7.5	More Details
CVE-2023-39786	Tenda AC8V4 V16.03.34.06 was discovered to contain a stack overflow via the time parameter in the sscanf function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39745	TP-Link TL-WR940N V2, TP-Link TL-WR941ND V5 and TP-Link TL-WR841N V8 were discovered to contain a buffer overflow via the component /userRpm/AccessCtrlAccessRulesRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	7.5	More Details
CVE-2023-20197	A vulnerability in the filesystem image parser for Hierarchical File System Plus (HFS+) of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an incorrect check for completion when a file is decompressed, which may result in a loop condition that could cause the affected software to stop responding. An attacker could exploit this vulnerability by submitting a crafted HFS+ filesystem image to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to stop responding, resulting in a DoS condition on the affected software and consuming available system resources. For a description of this vulnerability, see the ClamAV blog .	7.5	More Details
CVE-2023-40340	Jenkins NodeJS Plugin 1.6.0 and earlier does not properly mask (i.e., replace with asterisks) credentials specified in the Npm config file in Pipeline build logs.	7.5	More Details
CVE-2023-40339	Jenkins Config File Provider Plugin 952.va_544a_6234b_46 and earlier does not mask (i.e., replace with asterisks) credentials specified in configuration files when they're written to the build log.	7.5	More Details
CVE-2021-32421	dpic 2021.01.01 has a Heap Use-After-Free in thedeletestringbox() function in dpic.y.	7.5	More Details
CVE-2020-22570	Memcached 1.6.0 before 1.6.3 allows remote attackers to cause a denial of service (daemon crash) via a crafted meta command.	7.5	More Details
CVE-2023-40173	Social media skeleton is an uncompleted/framework social media project implemented using a php, css ,javascript and html. Prior to version 1.0.5 Social media skeleton did not properly salt passwords leaving user passwords susceptible to cracking should an attacker gain access to hashed passwords. This issue has been addressed in version 1.0.5 and users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2023-39748	An issue in the component /userRpm/NetworkCfgRpm of TP-Link TL-WR1041N V2 allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38976	An issue in weaviate v.1.20.0 allows a remote attacker to cause a denial of service via the handleUnbatchedGraphQLRequest function.	7.5	More Details
CVE-2023-20212	A vulnerability in the AutoIt module of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a logic error in the memory management of an affected device. An attacker could exploit this vulnerability by submitting a crafted AutoIt file to be scanned by ClamAV on the affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to restart unexpectedly, resulting in a DoS condition.	7.5	More Details
CVE-2022-43358	Stack overflow vulnerability in ast_selectors.cpp: in function Sass::ComplexSelector::has_placeholder in libsass:3.6.5-8-g210218, which can be exploited by attackers to cause a denial of service (DoS).	7.5	More Details
CVE-2020-22218	An issue was discovered in function _libssh2_packet_add in libssh2 1.10.0 allows attackers to access out of bounds memory.	7.5	More Details
CVE-2021-30047	VSFTPD 3.0.3 allows attackers to cause a denial of service due to limited number of connections allowed.	7.5	More Details
CVE-2022-43357	Stack overflow vulnerability in ast_selectors.cpp in function Sass::CompoundSelector::has_real_parent_ref in libsass:3.6.5-8-g210218, which can be exploited by attackers to causea denial of service (DoS). Also affects the command line driver for libsass, sassc 3.6.2.	7.5	More Details
CVE-2020-26652	An issue was discovered in function nl80211_send_chandef in rtl8812au v5.6.4.2 allows attackers to cause a denial of service.	7.5	More Details
CVE-2023-40735	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Cavo – Connecting for a Safer World BUTTERFLY BUTTON (Architecture flaw) allows loss of plausible deniability and confidentiality.This issue affects BUTTERFLY BUTTON: As of 2023-08-21.	7.5	More Details
CVE-2021-32420	dpic 2021.01.01 has a Heap-based Buffer Overflow in thestorestring function in dpic.y.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35342	GNU Binutils before 2.34 has an uninitialized-heap vulnerability in function tic4x_print_cond (file opcodes/tic4x-dis.c) which could allow attackers to make an information leak.	7.5	More Details
CVE-2023-40165	rubygems.org is the Ruby community's primary gem (library) hosting service. Insufficient input validation allowed malicious actors to replace any uploaded gem version that had a platform, version number, or gem name matching `/-\d/`, permanently replacing the legitimate upload in the canonical gem storage bucket, and triggering an immediate CDN purge so that the malicious gem would be served immediately. The maintainers have checked all gems matching the `/-\d/` pattern and can confirm that no unexpected `.gem`s were found. As a result, we believe this vulnerability was _not_ exploited. The easiest way to ensure that a user's applications were not exploited by this vulnerability is to check that all of your downloaded .gems have a checksum that matches the checksum recorded in the RubyGems.org database. RubyGems contributor Maciej Mensfeld wrote a tool to automatically check that all downloaded .gem files match the checksums recorded in the RubyGems.org database. You can use it by running: `bundle add bundler-integrity` followed by `bundle exec bundler-integrity`. Neither this tool nor anything else can prove you were not exploited, but the can assist your investigation by quickly comparing RubyGems API-provided checksums with the checksums of files on your disk. The issue has been patched with improved input validation and the changes are live. No action is required on the part of the user. Users are advised to validate their local gems.	7.4	More Details
CVE-2023-40168	TurboWarp is a desktop application that compiles scratch projects to JavaScript. TurboWarp Desktop versions prior to version 1.8.0 allowed a malicious project or custom extension to read arbitrary files from disk and upload them to a remote server. The only required user interaction is opening the sb3 file or loading the extension. The web version of TurboWarp is not affected. This bug has been addressed in commit `55e07e99b59` after an initial fix which was reverted. Users are advised to upgrade to version 1.8.0 or later. Users unable to upgrade should avoid opening sb3 files or loading extensions from untrusted sources.	7.4	More Details
CVE-2023-2316	Improper path handling in Typora before 1.6.7 on Windows and Linux allows a crafted webpage to access local files and exfiltrate them to remote web servers via "typora://app/<absolute-path>". This vulnerability can be exploited if a user opens a malicious markdown file in Typora, or copies text from a malicious webpage and paste it into Typora.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37426	EdgeConnect SD-WAN Orchestrator instances prior to the versions resolved in this advisory were found to have shared static SSH host keys for all installations. This vulnerability could allow an attacker to spoof the SSH host signature and thereby masquerade as a legitimate Orchestrator host.	7.4	More Details
CVE-2023-40175	Puma is a Ruby/Rack web server built for parallelism. Prior to versions 6.3.1 and 5.6.7, puma exhibited incorrect behavior when parsing chunked transfer encoding bodies and zero-length Content-Length headers in a way that allowed HTTP request smuggling. Severity of this issue is highly dependent on the nature of the web site using puma is. This could be caused by either incorrect parsing of trailing fields in chunked transfer encoding bodies or by parsing of blank/zero-length Content-Length headers. Both issues have been addressed and this vulnerability has been fixed in versions 6.3.1 and 5.6.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2023-4415	A vulnerability was found in Ruijie RG-EW1200G 07161417 r483. It has been rated as critical. Affected by this issue is some unknown functionality of the file /api/sys/login. The manipulation leads to improper authentication. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-237518 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2022-4894	Certain HP and Samsung Printer software packages may potentially be vulnerable to elevation of privilege due to Uncontrolled Search Path Element.	7.3	More Details
CVE-2023-32493	Dell PowerScale OneFS, 9.5.0.x, contains a protection mechanism bypass vulnerability. An unprivileged, remote attacker could potentially exploit this vulnerability, leading to denial of service, information disclosure and remote execution.	7.3	More Details
CVE-2023-31946	File Upload vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via a crafted PHP file to the artical.php.	7.2	More Details
CVE-2023-31945	SQL injection vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the id parameter at daily_expenditure_edit.php.	7.2	More Details
CVE-2023-39416	Proself Enterprise/Standard Edition Ver5.61 and earlier, Proself Gateway Edition Ver1.62 and earlier, and Proself Mail Sanitize Edition Ver1.07 and earlier allow a remote authenticated attacker with an administrative privilege to execute arbitrary OS commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31943	SQL injection vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the ticket_id parameter at ticket_detail.php.	7.2	More Details
CVE-2023-40352	McAfee Safe Connect before 2.16.1.126 may allow an adversary with system privileges to achieve privilege escalation by loading arbitrary DLLs.	7.2	More Details
CVE-2023-31944	SQL injection vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the emp_id parameter at employee_edit.php.	7.2	More Details
CVE-2023-31940	SQL injection vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the page_id parameter at article_edit.php.	7.2	More Details
CVE-2023-31941	File Upload vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via a crafted PHP file to the employee_insert.php.	7.2	More Details
CVE-2023-31938	SQL injection vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the emp_id parameter at employee_detail.php.	7.2	More Details
CVE-2023-34214	TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability stems from insufficient input validation in the certificate-generation function, which could potentially allow malicious users to execute remote code on affected devices.	7.2	More Details
CVE-2023-37428	A vulnerability in the EdgeConnect SD-WAN Orchestrator web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2023-33238	TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command injection vulnerability. This vulnerability stems from inadequate input validation in the certificate management function, which could potentially allow malicious users to execute remote code on affected devices.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34215	TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability stems from insufficient input validation and improper authentication in the certification-generation function, which could potentially allow malicious users to execute remote code on affected devices.	7.2	More Details
CVE-2023-31939	SQL injection vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the costomer_id parameter at customer_edit.php.	7.2	More Details
CVE-2023-37427	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability allows an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2022-44729	Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache XML Graphics Batik.This issue affects Apache XML Graphics Batik: 1.16. On version 1.16, a malicious SVG could trigger loading external resources by default, causing resource consumption or in some cases even information disclosure. Users are recommended to upgrade to version 1.17 or later.	7.1	More Details
CVE-2023-30779	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Jonathan Daggerhart Query Wrangler plugin <= 1.5.51 versions.	7.1	More Details
CVE-2023-31218	Cross-Site Request Forgery (CSRF) leading to Stored Cross-Site Scripting (XSS) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and Manager Professional plugin <= 1.0.6 versions.	7.1	More Details
CVE-2023-30782	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Andy Moyle Church Admin plugin <= 3.7.5 versions.	7.1	More Details
CVE-2023-32105	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ollybach WPPizza – A Restaurant Plugin plugin <= 3.17.1 versions.	7.1	More Details
CVE-2023-32106	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Fahad Mahmood WP Docs plugin <= 1.9.9 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32107	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Photo Gallery Team Photo Gallery by Ays – Responsive Image Gallery plugin <= 5.1.3 versions.	7.1	More Details
CVE-2023-30785	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Video Grid plugin <= 1.21 versions.	7.1	More Details
CVE-2023-32108	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ignazio Scimone Albo Pretorio On line plugin <= 4.6.3 versions.	7.1	More Details
CVE-2022-48541	A memory leak in ImageMagick 7.0.10-45 and 6.9.11-22 allows remote attackers to perform a denial of service via the "identify -help" command.	7.1	More Details
CVE-2023-32109	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ignazio Scimone Albo Pretorio On line plugin <= 4.6.3 versions.	7.1	More Details
CVE-2023-30871	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PT Woo Plugins (by Webdados) Stock Exporter for WooCommerce plugin <= 1.1.0 versions.	7.1	More Details
CVE-2023-30877	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Maxim Glazunov XML for Google Merchant Center plugin <= 3.0.1 versions.	7.1	More Details
CVE-2021-29390	libjpeg-turbo version 2.0.90 has a heap-based buffer over-read (2 bytes) in decompress_smooth_data in jdcoefct.c.	7.1	More Details
CVE-2023-40033	Flarum is an open source forum software. Flarum is affected by a vulnerability that allows an attacker to conduct a Blind Server-Side Request Forgery (SSRF) attack or disclose any file on the server, even with a basic user account on any Flarum forum. By uploading a file containing a URL and spoofing the MIME type, an attacker can manipulate the application to execute unintended actions. The vulnerability is due to the behavior of the `intervention/image` package, which attempts to interpret the supplied file contents as a URL, which then fetches its contents. This allows an attacker to exploit the vulnerability to perform SSRF attacks, disclose local file contents, or conduct a blind oracle attack. This has been patched in Flarum version 1.8.0. Users are advised to upgrade. Users unable to upgrade may disable PHP's `allow_url_fopen` which will prevent the fetching of external files via URLs as a temporary workaround for the SSRF aspect of the vulnerability.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20229	A vulnerability in the CryptoService function of Cisco Duo Device Health Application for Windows could allow an authenticated, local attacker with low privileges to conduct directory traversal attacks and overwrite arbitrary files on an affected system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by executing a directory traversal attack on an affected host. A successful exploit could allow an attacker to use a cryptographic key to overwrite arbitrary files with SYSTEM-level privileges, resulting in a denial of service (DoS) condition or data loss on the affected system.	7.1	More Details
CVE-2023-31094	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Lauri Karisola / WP Trio Stock Sync for WooCommerce plugin <= 2.4.0 versions.	7.1	More Details
CVE-2023-30499	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FolioVision FV Flowplayer Video Player plugin <= 7.5.32.7212 versions.	7.1	More Details
CVE-2023-28693	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Balasaheb Bhise Advanced Youtube Channel Pagination plugin <= 1.0 version.	7.1	More Details
CVE-2023-4387	A use-after-free flaw was found in vmxnet3_rq_alloc_rx_buf in drivers/net/vmxnet3/vmxnet3_drv.c in VMware's vmxnet3 ethernet NIC driver in the Linux Kernel. This issue could allow a local attacker to crash the system due to a double-free while cleaning up vmxnet3_rq_cleanup_all, which could also lead to a kernel information leak problem.	7.1	More Details
CVE-2023-40313	A BeanShell interpreter in remote server mode runs in OpenMNS Horizon versions earlier than 32.0.2 and in related Meridian versions which could allow arbitrary remote Java code execution. The solution is to upgrade to Meridian 2023.1.6, 2022.1.19, 2021.1.30, 2020.1.38 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.	7.1	More Details
CVE-2023-31071	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Yannick Lefebvre Modal Dialog plugin <= 3.5.14 versions.	7.1	More Details
CVE-2023-31076	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Really Simple Plugins Recipe Maker For Your Food Blog from Zip Recipes plugin <= 8.0.6 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31072	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Praveen Goswami Advanced Category Template plugin <= 0.1 versions.	7.1	More Details
CVE-2023-30473	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Maxim Glazunov YML for Yandex Market plugin <= 3.10.7 versions.	7.1	More Details
CVE-2023-26530	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Paul Kehrer Updraft plugin <= 0.6.1 versions.	7.1	More Details
CVE-2023-31074	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in hupe13 Extensions for Leaflet Map plugin <= 3.4.1 versions.	7.1	More Details
CVE-2023-37250	Unity Parsec has a TOCTOU race condition that permits local attackers to escalate privileges to SYSTEM if Parsec was installed in "Per User" mode. The application intentionally launches DLLs from a user-owned directory but intended to always perform integrity verification of those DLLs. This affects Parsec Loader versions through 8. Parsec Loader 9 is a fixed version.	7.0	More Details
CVE-2023-4389	A flaw was found in btrfs_get_root_ref in fs/btrfs/disk-io.c in the btrfs filesystem in the Linux Kernel due to a double decrement of the reference count. This issue may allow a local attacker with user privilege to crash the system or may lead to leaked internal kernel information.	7.0	More Details
CVE-2023-28075	Dell BIOS contain a Time-of-check Time-of-use vulnerability in BIOS. A local authenticated malicious user with physical access to the system could potentially exploit this vulnerability by using a specifically timed DMA transaction during an SMI in order to gain arbitrary code execution on the system.	6.9	More Details
CVE-2023-40174	Social media skeleton is an uncompleted/framework social media project implemented using a php, css ,javascript and html. Insufficient session expiration is a web application security vulnerability that occurs when a web application does not properly manage the lifecycle of a user's session. Social media skeleton releases prior to 1.0.5 did not properly limit manage user session lifecycles. This issue has been addressed in version 1.0.5 and users are advised to upgrade. There are no known workarounds for this vulnerability.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4212	A command injection vulnerability exists in Trane XL824, XL850, XL1050, and Pivot thermostats allowing an attacker to execute arbitrary commands as root using a specially crafted filename. The vulnerability requires physical access to the device via a USB stick.	6.8	More Details
CVE-2023-32490	Dell PowerScale OneFS 8.2x -9.5x contains an improper privilege management vulnerability. A high privilege local attacker could potentially exploit this vulnerability, leading to system takeover.	6.7	More Details
CVE-2023-34419	A buffer overflow has been identified in the SetupUtility driver in some Lenovo Notebook products which may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2023-27576	An issue was discovered in phpList before 3.6.14. Due to an access error, it was possible to manipulate and edit data of the system's super admin, allowing one to perform an account takeover of the user with super-admin permission. Specifically, for a request with updatepassword=1, a modified request (manipulating both the ID parameter and the associated username) can bypass the intended email confirmation requirement. For example, the attacker can start from an updatepassword=1 request with their own ID number, and change the ID number to 1 (representing the super admin account) and change the username to admin2. In the first step, the attacker changes the super admin's email address to one under the attacker's control. In the second step, the attacker performs a password reset for the super admin account. The new password allows login as the super admin, i.e., a successful account takeover.	6.7	More Details
CVE-2023-4028	A buffer overflow has been identified in the SystemUserMasterHddPwdDxe driver in some Lenovo Notebook products which may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2020-21583	An issue was discovered in hwclock.13-v2.27 allows attackers to gain escalated privlidges or execute arbitrary commands via the path parameter when setting the date.	6.7	More Details
CVE-2023-4029	A buffer overflow has been identified in the BoardUpdateAcpiDxe driver in some Lenovo ThinkPad products which may allow an attacker with local access and elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2023-4394	A use-after-free flaw was found in btrfs_get_dev_args_from_path in fs/btrfs/volumes.c in btrfs file-system in the Linux Kernel. This flaw allows a local attacker with special privileges to cause a system crash or leak internal kernel information	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38996	An issue in all versions of Douran DSGate allows a local authenticated privileged attacker to execute arbitrary code via the debug command.	6.7	More Details
CVE-2023-32494	Dell PowerScale OneFS, 8.0.x-9.5.x, contains an improper handling of insufficient privileges vulnerability. A local privileged attacker could potentially exploit this vulnerability, leading to elevation of privilege and affect in compliance mode also.	6.7	More Details
CVE-2023-32486	Dell PowerScale OneFS 9.5.x version contain a privilege escalation vulnerability. A low privilege local attacker could potentially exploit this vulnerability, leading to escalation of privileges.	6.7	More Details
CVE-2023-32489	Dell PowerScale OneFS 8.2x -9.5x contains a privilege escalation vulnerability. A local attacker with high privileges could potentially exploit this vulnerability, to bypass mode protections and gain elevated privileges.	6.7	More Details
CVE-2023-38734	IBM Robotic Process Automation 21.0.0 through 21.0.7.1 and 23.0.0 through 23.0.1 is vulnerable to incorrect privilege assignment when importing users from an LDAP directory. IBM X-Force ID: 262481.	6.6	More Details
CVE-2023-37432	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2023-40345	Jenkins Delphix Plugin 3.0.2 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Overall/Read permission to access and capture credentials they are not entitled to.	6.5	More Details
CVE-2020-22524	Buffer Overflow vulnerability in FreeImage_Load function in FreeImage Library 3.19.0(r1828) allows attackers to cuase a denial of service via crafted PFM file.	6.5	More Details
CVE-2023-4455	Cross-Site Request Forgery (CSRF) in GitHub repository wallabag/wallabag prior to 2.6.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37429	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2023-37431	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2023-37430	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2023-37433	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2021-46310	An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.	6.5	More Details
CVE-2023-37434	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37435	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2020-19185	Buffer Overflow vulnerability in one_one_mapping function in progs/dump_entry.c:1373 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	6.5	More Details
CVE-2020-19186	Buffer Overflow vulnerability in _nc_find_entry function in tinfo/comp_hash.c:66 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	6.5	More Details
CVE-2020-19187	Buffer Overflow vulnerability in fmt_entry function in progs/dump_entry.c:1100 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	6.5	More Details
CVE-2020-19188	Buffer Overflow vulnerability in fmt_entry function in progs/dump_entry.c:1116 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	6.5	More Details
CVE-2020-18652	Buffer Overflow vulnerability in WEBP_Support.cpp in exempi 2.5.0 and earlier allows remote attackers to cause a denial of service via opening of crafted webp file.	6.5	More Details
CVE-2020-18651	Buffer Overflow vulnerability in function ID3_Support::ID3v2Frame::getFrameValue in exempi 2.5.0 and earlier allows remote attackers to cause a denial of service via opening of crafted audio file with ID3V2 frame.	6.5	More Details
CVE-2020-18382	Heap-buffer-overflow in /src/wasm/wasm-binary.cpp in wasm::WasmBinaryBuilder::visitBlock(wasm::Block*) in Binaryen 1.38.26. A crafted wasm input can cause a segmentation fault, leading to denial-of-service, as demonstrated by wasm-opt.	6.5	More Details
CVE-2020-18378	A NULL pointer dereference was discovered in SExpressionWasmBuilder::makeBlock in wasm/wasm-s-parser.c in Binaryen 1.38.26. A crafted wasm input can cause a segmentation fault, leading to denial-of-service, as demonstrated by wasm-as.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38909	An issue in TPLink Smart Bulb Tapo series L530 before 1.2.4, L510E before 1.1.0, L630 before 1.0.4, P100 before 1.5.0, and Tapo Application 2.8.14 allows a remote attacker to obtain sensitive information via the IV component in the AES128-CBC function.	6.5	More Details
CVE-2023-38908	An issue in TPLink Smart Bulb Tapo series L530 before 1.2.4, L510E before 1.1.0, L630 before 1.0.4, P100 before 1.5.0, and Tapo Application 2.8.14 allows a remote attacker to obtain sensitive information via the TSKEP authentication function.	6.5	More Details
CVE-2023-38906	An issue in TPLink Smart Bulb Tapo series L530 1.1.9, L510E 1.0.8, L630 1.0.3, P100 1.4.9, Smart Camera Tapo series C200 1.1.18, and Tapo Application 2.8.14 allows a remote attacker to obtain sensitive information via the authentication code for the UDP message.	6.5	More Details
CVE-2020-19189	Buffer Overflow vulnerability in postprocess_terminfo function in tinfo/parse_entry.c:997 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	6.5	More Details
CVE-2020-19190	Buffer Overflow vulnerability in _nc_find_entry in tinfo/comp_hash.c:70 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command.	6.5	More Details
CVE-2023-30784	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Kaya Studio Kaya QR Code Generator plugin <= 1.5.2 versions.	6.5	More Details
CVE-2023-40347	Jenkins Maven Artifact ChoiceListProvider (Nexus) Plugin 1.14 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to.	6.5	More Details
CVE-2023-4417	Improper access controls in the entry duplication component in Devolutions Remote Desktop Manager 2023.2.19 and earlier versions on Windows allows an authenticated user, under specific circumstances, to inadvertently share their personal vault entry with shared vaults via an incorrect vault in the duplication write process.	6.5	More Details
CVE-2023-37438	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37437	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2023-37436	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.5	More Details
CVE-2020-22628	Buffer Overflow vulnerability in LibRaw::stretch() function in libraw\src\postprocessing\aspect_ratio.cpp.	6.5	More Details
CVE-2023-20209	A vulnerability in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker with read-write privileges on the application to perform a command injection attack that could result in remote code execution on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to establish a remote shell with root privileges.	6.5	More Details
CVE-2023-40037	Apache NiFi 1.21.0 through 1.23.0 support JDBC and JNDI JMS access in several Processors and Controller Services with connection URL validation that does not provide sufficient protection against crafted inputs. An authenticated and authorized user can bypass connection URL validation using custom input formatting. The resolution enhances connection URL validation and introduces validation for additional related properties. Upgrading to Apache NiFi 1.23.1 is the recommended mitigation.	6.5	More Details
CVE-2022-37051	An issue was discovered in Poppler 22.07.0. There is a reachable abort which leads to denial of service because the main function in pdfunite.cc lacks a stream check before saving an embedded file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20221	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based management interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform a factory reset of the affected device, resulting in a Denial of Service (DoS) condition.	6.5	More Details
CVE-2023-20111	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access sensitive information. This vulnerability is due to the improper storage of sensitive information within the web-based management interface. An attacker could exploit this vulnerability by logging in to the web-based management interface and viewing hidden fields within the application. A successful exploit could allow the attacker to access sensitive information, including device entry credentials, that could aid the attacker in further attacks.	6.5	More Details
CVE-2020-24294	Buffer Overflow vulnerability in psdParser::UnpackRLE function in PSDParser.cpp in FreeImage 3.19.0 [r1859] allows remote attackers to cuase a denial of service via opening of crafted psd file.	6.5	More Details
CVE-2023-20017	Multiple vulnerabilities in Cisco Intersight Private Virtual Appliance could allow an authenticated, remote attacker to execute arbitrary commands using root-level privileges. The attacker would need to have Administrator privileges on the affected device to exploit these vulnerabilities. These vulnerabilities are due to insufficient input validation when extracting uploaded software packages. An attacker could exploit these vulnerabilities by authenticating to an affected device and uploading a crafted software package. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20013	Multiple vulnerabilities in Cisco Intersight Private Virtual Appliance could allow an authenticated, remote attacker to execute arbitrary commands using root-level privileges. The attacker would need to have Administrator privileges on the affected device to exploit these vulnerabilities. These vulnerabilities are due to insufficient input validation when extracting uploaded software packages. An attacker could exploit these vulnerabilities by authenticating to an affected device and uploading a crafted software package. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.	6.5	More Details
CVE-2022-40090	An issue was discovered in function TIFFReadDirectory libtiff before 4.4.0 allows attackers to cause a denial of service via crafted TIFF file.	6.5	More Details
CVE-2022-38349	An issue was discovered in Poppler 22.08.0. There is a reachable assertion in Object.h, will lead to denial of service because PDFDoc::replacePageDict in PDFDoc.cc lacks a stream check before saving an embedded file.	6.5	More Details
CVE-2023-29387	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Julien Crego Manager for Icomoon plugin <= 2.0 versions.	6.5	More Details
CVE-2022-48564	read_ints in plistlib.py in Python through 3.9.1 is vulnerable to a potential DoS attack via CPU and RAM exhaustion when processing malformed Apple Property List files in binary format.	6.5	More Details
CVE-2023-32103	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Theme Palace TP Education plugin <= 4.4 versions.	6.5	More Details
CVE-2022-37052	A reachable Object::getString assertion in Poppler 22.07.0 allows attackers to cause a denial of service due to a failure in markObject.	6.5	More Details
CVE-2022-37050	In Poppler 22.07.0, PDFDoc::savePageAs in PDFDoc.c callows attackers to cause a denial-of-service (application crashes with SIGABRT) by crafting a PDF file in which the xref data structure is mishandled in getCatalog processing. Note that this vulnerability is caused by the incomplete patch of CVE-2018-20662.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40172	Social media skeleton is an uncompleted/framework social media project implemented using a php, css ,javascript and html. A Cross-site request forgery (CSRF) attack is a type of malicious attack whereby an attacker tricks a victim into performing an action on a website that they do not intend to do. This can be done by sending the victim a malicious link or by exploiting a vulnerability in the website. Prior to version 1.0.5 Social media skeleton did not properly restrict CSRF attacks. This has been addressed in version 1.0.5 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-31079	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Chris Roberts Tippy plugin <= 6.2.1 versions.	6.5	More Details
CVE-2023-23563	An issue was discovered in Geomatika IsiGeo Web 6.0. It allows remote authenticated users to obtain sensitive database content via SQL Injection.	6.5	More Details
CVE-2023-31492	Zoho ManageEngine ADManager Plus version 7182 and prior disclosed the default passwords for the account restoration of unauthorized domains to the authenticated users.	6.5	More Details
CVE-2021-40262	A stack exhaustion issue was discovered in FreeImage before 1.18.0 via the Validate function in PluginRAW.cpp.	6.5	More Details
CVE-2021-40264	NULL pointer dereference vulnerability in FreeImage before 1.18.0 via the FreeImage_CloneTag function inFreeImageTag.cpp.	6.5	More Details
CVE-2021-46312	An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cause a denial of service via divide by zero.	6.5	More Details
CVE-2021-40266	FreeImage before 1.18.0, ReadPalette function in PluginTIFF.cpp is vulnerabile to null pointer dereference.	6.5	More Details
CVE-2021-43171	Improper verification of applications' cryptographic signatures in the /e/OS app store client App Lounge before 0.19q allows attackers in control of the application server to install malicious applications on user's systems by altering the server's API response.	6.5	More Details
CVE-2021-46179	Reachable Assertion vulnerability in upx before 4.0.0 allows attackers to cause a denial of service via crafted file passed to the the readx function.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18839	Buffer Overflow vulnerability in HtmlOutputDev::page in poppler 0.75.0 allows attackers to cause a denial of service.	6.5	More Details
CVE-2020-35357	A buffer overflow can occur when calculating the quantile value using the Statistics Library of GSL (GNU Scientific Library), versions 2.5 and 2.6. Processing a maliciously crafted input data for gsl_stats_quantile_from_sorted_data of the library may lead to unexpected application termination or arbitrary code execution.	6.5	More Details
CVE-2023-29182	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiOS before 7.0.3 allows a privileged attacker to execute arbitrary code via specially crafted CLI commands, provided the attacker were able to evade FortiOS stack protections.	6.4	More Details
CVE-2023-24517	Unrestricted Upload of File with Dangerous Type vulnerability in the Pandora FMS File Manager component, allows an attacker to make make use of this issue (unrestricted file upload) to execute arbitrary system commands. This issue affects Pandora FMS v767 version and prior versions on all platforms.	6.4	More Details
CVE-2023-24514	Cross-site Scripting (XSS) vulnerability in Visual Console Module of Pandora FMS could be used to hijack admin users session cookie values, carry out phishing attacks, etc. This issue affects Pandora FMS v767 version and prior versions on all platforms.	6.3	More Details
CVE-2023-4407	A vulnerability classified as critical was found in Codecanyon Credit Lite 1.5.4. Affected by this vulnerability is an unknown functionality of the file /portal/reports/account_statement of the component POST Request Handler. The manipulation of the argument date1/date2 leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-237511.	6.3	More Details
CVE-2023-4443	A vulnerability classified as critical has been found in SourceCodester Free Hospital Management System for Small Practices 1.0/5.0.12. Affected is an unknown function of the file vm\doctor\edit-doc.php. The manipulation of the argument id00/nic/oldemail/email/spec/Tele 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-237564.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4444	A vulnerability classified as critical was found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected by this vulnerability is an unknown functionality of the file vm\patient\edit-user.php. The manipulation of the argument id00/nic/oldemail/email/spec/Tele leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-237565 was assigned to this vulnerability.	6.3	More Details
CVE-2023-4445	A vulnerability, which was classified as critical, has been found in Mini-Tmall up to 20230811. Affected by this issue is some unknown functionality of the file product/1/1?test=1&test2=2&. The manipulation of the argument orderBy leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-237566 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4442	A vulnerability was found in SourceCodester Free Hospital Management System for Small Practices 1.0. It has been rated as critical. This issue affects some unknown processing of the file \vm\patient\booking-complete.php. The manipulation of the argument userid/apponum/scheduleid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-237563.	6.3	More Details
CVE-2023-4447	A vulnerability has been found in OpenRapid RapidCMS 1.3.1 and classified as critical. This vulnerability affects unknown code of the file admin/article-chat.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-237568.	6.3	More Details
CVE-2023-4448	A vulnerability was found in OpenRapid RapidCMS 1.3.1 and classified as critical. This issue affects some unknown processing of the file admin/run-movepass.php. The manipulation of the argument password/password2 leads to weak password recovery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 4dff387283060961c362d50105ff8da8ea40bcbe. It is recommended to apply a patch to fix this issue. The identifier VDB-237569 was assigned to this vulnerability.	6.3	More Details
CVE-2023-4449	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /index.php?page=member. The manipulation of the argument columns[0][data] 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-237570 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4441	A vulnerability was found in SourceCodester Free Hospital Management System for Small Practices 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /patient/appointment.php. The manipulation of the argument sheduledate leads to sql injection. The attack can be initiated remotely. VDB-237562 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4450	A vulnerability was found in jeecgboot JimuReport up to 1.6.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Template Handler. The manipulation leads to injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.6.1 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-237571.	6.3	More Details
CVE-2023-4438	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file app/ajax/search_sales_report.php. The manipulation of the argument customer 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-237559.	6.3	More Details
CVE-2023-4437	A vulnerability, which was classified as critical, was found in SourceCodester Inventory Management System 1.0. Affected is an unknown function of the file app/ajax/search_sell_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-237558 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4436	A vulnerability, which was classified as critical, has been found in SourceCodester Inventory Management System 1.0. This issue affects some unknown processing of the file app/action/edit_update.php. The manipulation of the argument user_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-237557 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4409	A vulnerability, which was classified as critical, has been found in NBS&HappySoftWeChat 1.1.6. Affected by this issue is some unknown functionality. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-237512.	6.3	More Details
CVE-2023-32491	Dell PowerScale OneFS 9.5.0.x, contains an insertion of sensitive information into log file vulnerability in SNMPv3. A low privileges user could potentially exploit this vulnerability, leading to information disclosure.	6.3	More Details
CVE-2023-4410	A vulnerability, which was classified as critical, was found in TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023. This affects the function setDiagnosisCfg. The manipulation 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 identifier VDB-237513 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4411	A vulnerability has been found in TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 and classified as critical. This vulnerability affects the function setTracerouteCfg. The manipulation leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-237514 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4412	A vulnerability was found in TOTOLINK EX1200L EN_V9.3.5u.6146_B20201023 and classified as critical. This issue affects the function setWanCfg. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-237515. 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-2023-4414	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20230807. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-237517 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2971	Improper path handling in Typora before 1.7.0-dev on Windows and Linux allows a crafted webpage to access local files and exfiltrate them to remote web servers via "typora://app/typemark/". This vulnerability can be exploited if a user opens a malicious markdown file in Typora, or copies text from a malicious webpage and paste it into Typora.	6.3	More Details
CVE-2023-4440	A vulnerability was found in SourceCodester Free Hospital Management System for Small Practices 1.0. It has been classified as critical. This affects an unknown part of the file appointment.php. The manipulation of the argument sheduledate leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-237561 was assigned to this vulnerability.	6.3	More Details
CVE-2022-44215	There is an open redirect vulnerability in Titan FTP server 19.0 and below. Users are redirected to any target URL.	6.1	More Details
CVE-2020-23992	Cross Site Scripting (XSS) in Nagios XI 5.7.1 allows remote attackers to run arbitrary code via returnUrl parameter in a crafted GET request.	6.1	More Details
CVE-2020-22181	A reflected cross site scripting (XSS) vulnerability was discovered on Samsung sww-3400rw Router devices via the m2 parameter of the sess-bin/command.cgi	6.1	More Details
CVE-2022-48547	A reflected cross-site scripting (XSS) vulnerability in Cacti 0.8.7g and earlier allows unauthenticated remote attackers to inject arbitrary web script or HTML in the "ref" parameter at auth_changepassword.php.	6.1	More Details
CVE-2023-37439	Multiple vulnerabilities in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the EdgeConnect SD-WAN Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to the exposure and corruption of sensitive data controlled by the EdgeConnect SD-WAN Orchestrator host.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45582	Open Redirect vulnerability in Horizon Web Dashboard 19.4.0 thru 20.1.4 via the success_url parameter.	6.1	More Details
CVE-2022-41444	Cross Site Scripting (XSS) vulnerability in Cacti 1.2.21 via crafted POST request to graphs_new.php.	6.1	More Details
CVE-2023-26140	Versions of the package @excalidraw/excalidraw from 0.0.0 are vulnerable to Cross-site Scripting (XSS) via embedded links in whiteboard objects due to improper input sanitization.	6.1	More Details
CVE-2023-4434	Missing Authorization in GitHub repository hamza417/inure prior to build88.	6.1	More Details
CVE-2023-20228	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.	6.1	More Details
CVE-2023-2272	The Tiempo.com WordPress plugin through 0.1.2 does not sanitise and escape the page parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-4451	Cross-site Scripting (XSS) - Reflected in GitHub repository cockpit-hq/cockpit prior to 2.6.4.	6.1	More Details
CVE-2023-3936	The Blog2Social WordPress plugin before 7.2.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-3954	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.15.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39971	Improper Neutralization of Input During Web Page Generation vulnerability in AcyMailing Enterprise component for Joomla allows XSS. This issue affects AcyMailing Enterprise component for Joomla: 6.7.0-8.6.3.	6.1	More Details
CVE-2023-4432	Cross-site Scripting (XSS) - Reflected in GitHub repository cockpit-hq/cockpit prior to 2.6.4.	6.1	More Details
CVE-2023-39543	Cross-site scripting vulnerability in LuxCal Web Calendar prior to 5.2.3M (MySQL version) and LuxCal Web Calendar prior to 5.2.3L (SQLite version) allows a remote unauthenticated attacker to execute an arbitrary script on the web browser of the user who is using the product.	6.1	More Details
CVE-2023-1465	The WP EasyPay WordPress plugin before 4.1 does not escape some generated URLs before outputting them back in pages, leading to Reflected Cross-Site Scripting issues which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-0058	The Tiempo.com WordPress plugin through 0.1.2 does not have CSRF check when creating and editing its shortcode, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	6.1	More Details
CVE-2023-2122	The Image Optimizer by 10web WordPress plugin before 1.0.27 does not sanitise and escape the iowd_tabs_active parameter before rendering it in the plugin admin panel, leading to a reflected Cross-Site Scripting vulnerability, allowing an attacker to trick a logged in admin to execute arbitrary javascript by clicking a link.	6.1	More Details
CVE-2023-39507	Improper authorization in the custom URL scheme handler in "Rikunabi NEXT" App for Android prior to ver. 11.5.0 allows a malicious intent to lead the vulnerable App to access an arbitrary website.	6.1	More Details
CVE-2023-38910	CSZ CMS 1.3.0 is vulnerable to cross-site scripting (XSS), which allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered in the 'Carousel Wiget' section and choosing our carousel widget created above, in 'Photo URL' and 'YouTube URL' plugin.	6.1	More Details
CVE-2023-2123	The WP Inventory Manager WordPress plugin before 2.1.0.13 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40252	Improper Control of Generation of Code ('Code Injection') vulnerability in Genians Genian NAC V4.0, Genians Genian NAC V5.0, Genians Genian NAC Suite V5.0, Genians Genian ZTNA allows Replace Trusted Executable.This issue affects Genian NAC V4.0: from V4.0.0 through V4.0.155; Genian NAC V5.0: from V5.0.0 through V5.0.42 (Revision 117460); Genian NAC Suite V5.0: from V5.0.0 through V5.0.54; Genian ZTNA: from V6.0.0 through V6.0.15.	6.0	More Details
CVE-2020-22217	Buffer overflow vulnerability in c-ares before 1_16_1 thru 1_17_0 via function ares_parse_soa_reply in ares_parse_soa_reply.c.	5.9	More Details
CVE-2023-30876	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Dave Ross Dave's WordPress Live Search plugin <= 4.8.1 versions.	5.9	More Details
CVE-2023-30874	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Steve Curtis, St. Pete Design Gps Plotter plugin <= 5.1.4 versions.	5.9	More Details
CVE-2023-31091	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pradeep Singh Dynamically Register Sidebars plugin <= 1.0.1 versions.	5.9	More Details
CVE-2023-28690	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Steinbrecher WP BrowserUpdate plugin <= 4.5 versions.	5.9	More Details
CVE-2023-28783	Auth. (shop manager+) Stored Cross-Site Scripting (XSS) vulnerability in PHPRADAR Woocommerce Tip/Donation plugin <= 1.2 versions.	5.9	More Details
CVE-2023-28533	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in M Williams Cab Grid plugin <= 1.5.15 versions.	5.9	More Details
CVE-2023-30875	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in All My Web Needs Logo Scheduler plugin <= 1.2.0 versions.	5.9	More Details
CVE-2023-31228	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CreativeMindsSolutions CM On Demand Search And Replace plugin <= 1.3.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31232	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David Artiss Plugins List plugin <= 2.5 versions.	5.9	More Details
CVE-2023-28622	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in Trident Technolabs Easy Slider Revolution plugin <= 1.0.0 versions.	5.9	More Details
CVE-2023-32130	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Daniel Powney Multi Rating plugin <= 5.0.6 versions.	5.9	More Details
CVE-2023-38737	IBM WebSphere Application Server Liberty 22.0.0.13 through 23.0.0.7 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 262567.	5.9	More Details
CVE-2022-48566	An issue was discovered in compare_digest in Lib/hmac.py in Python through 3.9.1. Constant-time-defeating optimisations were possible in the accumulator variable in hmac.compare_digest.	5.9	More Details
CVE-2023-40343	Jenkins Tuleap Authentication Plugin 1.1.20 and earlier uses a non-constant time comparison function when validating an authentication token allowing attackers to use statistical methods to obtain a valid authentication token.	5.9	More Details
CVE-2023-30786	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Benjamin Guy Captcha Them All plugin <= 1.3.3 versions.	5.9	More Details
CVE-2023-24516	Cross-site Scripting (XSS) vulnerability in the Pandora FMS Special Days component allows an attacker to use it to steal the session cookie value of admin users easily with little user interaction. This issue affects Pandora FMS v767 version and prior versions on all platforms.	5.9	More Details
CVE-2023-32122	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Spiffy Plugins Spiffy Calendar plugin <= 4.9.3 versions.	5.8	More Details
CVE-2023-4456	A flaw was found in openshift-logging LokiStack. The key used for caching is just the token, which is too broad. This issue allows a user with a token valid for one action to execute other actions as long as the authorization allowing the original action is still cached.	5.7	More Details
CVE-2023-3481	Critters versions 0.0.17-0.0.19 have an issue when parsing the HTML, which leads to a potential cross-site scripting (XSS) bug. We recommend upgrading to version 0.0.20 of the extension.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4454	Cross-Site Request Forgery (CSRF) in GitHub repository wallabag/wallabag prior to 2.6.3.	5.7	More Details
CVE-2023-2737	Improper log permissions in SafeNet Authentication Service Version 3.4.0 on Windows allows an authenticated attacker to cause a denial of service via local privilege escalation.	5.7	More Details
CVE-2022-48554	File before 5.43 has an stack-based buffer over-read in file_copystr in funcs.c. NOTE: "File" is the name of an Open Source project.	5.5	More Details
CVE-2022-48545	An infinite recursion in Catalog::findDestInTree can cause denial of service for xpdf 4.02.	5.5	More Details
CVE-2022-48065	GNU Binutils before 2.40 was discovered to contain a memory leak vulnerability var the function find_abstract_instance in dwarf2.c.	5.5	More Details
CVE-2022-48064	GNU Binutils before 2.40 was discovered to contain an excessive memory consumption vulnerability via the function bfd_dwarf2_find_nearest_line_with_alt at dwarf2.c. The attacker could supply a crafted ELF file and cause a DNS attack.	5.5	More Details
CVE-2022-47011	An issue was discovered function parse_stab_struct_fields in stabs.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	5.5	More Details
CVE-2022-48063	GNU Binutils before 2.40 was discovered to contain an excessive memory consumption vulnerability via the function load_separate_debug_files at dwarf2.c. The attacker could supply a crafted ELF file and cause a DNS attack.	5.5	More Details
CVE-2022-29654	Buffer overflow vulnerability in quote_for_pmake in asm/nasm.c in nasm before 2.15.05 allows attackers to cause a denial of service via crafted file.	5.5	More Details
CVE-2023-39741	lrzip v0.651 was discovered to contain a heap overflow via the libzpaq::PostProcessor::write(int) function at /libzpaq/libzpaq.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38905	SQL injection vulnerability in Jeecg-boot v.3.5.0 and before allows a local attacker to cause a denial of service via the Benchmark, PG_Sleep, DBMS_Lock.Sleep, Waitfor, DECODE, and DBMS_PIPE.RECEIVE_MESSAGE functions.	5.5	More Details
CVE-2022-47010	An issue was discovered function pr_function_type in prdbg.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	5.5	More Details
CVE-2022-47008	An issue was discovered function make_tempdir, and make_tempname in bucomm.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	5.5	More Details
CVE-2022-47007	An issue was discovered function stab_demangle_v3_arg in stabs.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks.	5.5	More Details
CVE-2023-20217	A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient input validation by the operating system CLI. An attacker could exploit this vulnerability by issuing certain commands using sudo. A successful exploit could allow the attacker to view arbitrary files as root on the underlying operating system. The attacker must have valid credentials on the affected device.	5.5	More Details
CVE-2020-18780	A Use After Free vulnerability in function new_Token in asm/preproc.c in nasm 2.14.02 allows attackers to cause a denial of service via crafted nasm command.	5.5	More Details
CVE-2022-35206	Null pointer dereference vulnerability in Binutils readelf 2.38.50 via function read_and_display_attr_value in file dwarf.c.	5.5	More Details
CVE-2022-35205	An issue was discovered in Binutils readelf 2.38.50, reachable assertion failure in function display_debug_names allows attackers to cause a denial of service.	5.5	More Details
CVE-2020-18781	Heap buffer overflow vulnerability in FilePOSIX::read in File.cpp in audiofile 0.3.6 may cause denial-of-service via a crafted wav file, this bug can be triggered by the executable sfconvert.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27471	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. UEFI implementations do not correctly protect and validate information contained in the 'MeSetup' UEFI variable. On some systems, this variable can be overwritten using operating system APIs. Exploitation of this vulnerability could potentially lead to denial of service for the platform.	5.5	More Details
CVE-2020-21896	A Use After Free vulnerability in svg_dev_text_span_as_paths_defs function in source/fitz/svg-device.c in Artifex Software MuPDF 1.16.0 allows remote attackers to cause a denial of service via opening of a crafted PDF file.	5.5	More Details
CVE-2023-38666	Bento4 v1.6.0-639 was discovered to contain a segmentation violation via the AP4_Processor::ProcessFragments function in mp4encrypt.	5.5	More Details
CVE-2020-21723	A Segmentation Fault issue discovered StreamSerializer::extractStreams function in streamSerializer.cpp in oggvideotools 0.9.1 allows remote attackers to cause a denial of service (crash) via opening of crafted ogg file.	5.5	More Details
CVE-2020-21710	A divide by zero issue discovered in eps_print_page in gdevepsn.c in Artifex Software GhostScript 9.50 allows remote attackers to cause a denial of service via opening of crafted PDF file.	5.5	More Details
CVE-2023-38667	Stack-based buffer over-read in function disasm in nasm 2.16 allows attackers to cause a denial of service.	5.5	More Details
CVE-2020-21687	Buffer Overflow vulnerability in scan function in stdscan.c in nasm 2.15rc0 allows remote attackers to cause a denial of service via crafted asm file.	5.5	More Details
CVE-2020-26683	A memory leak issue discovered in /pdf/pdf-font-add.c in Artifex Software MuPDF 1.17.0 allows attackers to obtain sensitive information.	5.5	More Details
CVE-2020-21686	A stack-use-after-scope issue discovered in expand_mmac_params function in preproc.c in nasm before 2.15.04 allows remote attackers to cause a denial of service via crafted asm file.	5.5	More Details
CVE-2020-21685	Buffer Overflow vulnerability in hash_findi function in hashtbl.c in nasm 2.15rc0 allows remote attackers to cause a denial of service via crafted asm file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21679	Buffer Overflow vulnerability in WritePCXImage function in pcx.c in GraphicsMagick 1.4 allows remote attackers to cause a denial of service via converting of crafted image file to pcx format.	5.5	More Details
CVE-2023-38668	Stack-based buffer over-read in disasm in nasm 2.16 allows attackers to cause a denial of service (crash).	5.5	More Details
CVE-2020-21528	A Segmentation Fault issue discovered in in ieee_segment function in outieee.c in nasm 2.14.03 and 2.15 allows remote attackers to cause a denial of service via crafted assembly file.	5.5	More Details
CVE-2020-21490	An issue was discovered in GNU Binutils 2.34. It is a memory leak when process microblaze-dis.c. This one will consume memory on each insn disassembled.	5.5	More Details
CVE-2020-21047	The libcpu component which is used by libasm of elfutils version 0.177 (git 47780c9e), suffers from denial-of-service vulnerability caused by application crashes due to out-of-bounds write (CWE-787), off-by-one error (CWE-193) and reachable assertion (CWE-617); to exploit the vulnerability, the attackers need to craft certain ELF files which bypass the missing bound checks.	5.5	More Details
CVE-2023-4459	A NULL pointer dereference flaw was found in vmxnet3_rq_cleanup in drivers/net/vmxnet3/vmxnet3_drv.c in the networking sub-component in vmxnet3 in the Linux Kernel. This issue may allow a local attacker with normal user privilege to cause a denial of service due to a missing sanity check during cleanup.	5.5	More Details
CVE-2020-19724	A memory consumption issue in get_data function in binutils/nm.c in GNU nm before 2.34 allows attackers to cause a denial of service via crafted command.	5.5	More Details
CVE-2020-18768	There exists one heap buffer overflow in _TIFFmemcpy in tif_unix.c in libtiff 4.0.10, which allows an attacker to cause a denial-of-service through a crafted tiff file.	5.5	More Details
CVE-2020-18770	An issue was discovered in function zzip_disk_entry_to_file_header in mmapped.c in zziplib 0.13.69, which will lead to a denial-of-service.	5.5	More Details
CVE-2023-38665	Null pointer dereference in ieee_write_file in nasm 2.16rc0 allows attackers to cause a denial of service (crash).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4385	A NULL pointer dereference flaw was found in dbFree in fs/jfs/jfs_dmap.c in the journaling file system (JFS) in the Linux Kernel. This issue may allow a local attacker to crash the system due to a missing sanity check.	5.5	More Details
CVE-2023-4446	A vulnerability, which was classified as critical, was found in OpenRapid RapidCMS 1.3.1. This affects an unknown part of the file template/default/category.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-237567.	5.5	More Details
CVE-2020-22916	An issue discovered in XZ 5.2.5 allows attackers to cause a denial of service via decompression of a crafted file. NOTE: the vendor disputes the claims of "endless output" and "denial of service" because decompression of the 17,486 bytes always results in 114,881,179 bytes, which is often a reasonable size increase.	5.5	More Details
CVE-2023-4435	Improper Input Validation in GitHub repository hamza417/inure prior to build88.	5.5	More Details
CVE-2023-37440	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an unauthenticated remote attacker to conduct a server-side request forgery (SSRF) attack. A successful exploit allows an attacker to enumerate information about the internal structure of the EdgeConnect SD-WAN Orchestrator host leading to potential disclosure of sensitive information.	5.5	More Details
CVE-2023-4453	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.6.8.	5.4	More Details
CVE-2023-40342	Jenkins Flaky Test Handler Plugin 1.2.2 and earlier does not escape JUnit test contents when showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control JUnit report file contents.	5.4	More Details
CVE-2023-40350	Jenkins Docker Swarm Plugin 1.11 and earlier does not escape values returned from Docker before inserting them into the Docker Swarm Dashboard view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control responses from Docker.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40068	Cross-site scripting vulnerability in Advanced Custom Fields versions 6.1.0 to 6.1.7 and Advanced Custom Fields Pro versions 6.1.0 to 6.1.7 allows a remote authenticated attacker to execute an arbitrary script on the web browser of the user who is logging in to the product with the administrative privilege.	5.4	More Details
CVE-2023-1110	The Yellow Yard Searchbar WordPress plugin before 2.8.12 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-4204	NPort IAW5000A-I/O Series firmware version v2.2 and prior is affected by a hardcoded credential vulnerabilitywhich poses a potential risk to the security and integrity of the affected device. This vulnerability is attributed to the presence of a hardcoded key, which could potentially facilitate firmware manipulation.	5.4	More Details
CVE-2023-40346	Jenkins Shortcut Job Plugin 0.4 and earlier does not escape the shortcut redirection URL, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure shortcut jobs.	5.4	More Details
CVE-2023-0551	The REST API TO MiniProgram WordPress plugin through 4.6.1 does not have authorisation and CSRF checks in an AJAX action, allowing ay authenticated users, such as subscriber to call and delete arbitrary attachments	5.4	More Details
CVE-2023-35011	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 257705.	5.4	More Details
CVE-2023-38904	A Cross Site Scripting (XSS) vulnerability in Netlify CMS v.2.10.192 allows a remote attacker to execute arbitrary code via a crafted payload to the body parameter of the new post function.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20205	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid credentials to access the web-based management interface of the affected device.	5.4	More Details
CVE-2023-39599	Cross-Site Scripting (XSS) vulnerability in CSZ CMS v.1.3.0 allows attackers to execute arbitrary code via a crafted payload to the Social Settings parameter.	5.4	More Details
CVE-2023-4395	Cross-site Scripting (XSS) - Stored in GitHub repository cockpit-hq/cockpit prior to 2.6.4.	5.4	More Details
CVE-2023-0274	The URL Params WordPress plugin before 2.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4782	The ClickFunnels WordPress plugin through 3.1.1 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2023-4433	Cross-site Scripting (XSS) - Stored in GitHub repository cockpit-hq/cockpit prior to 2.6.4.	5.4	More Details
CVE-2023-39094	Cross Site Scripting vulnerability in ZeroWdd studentmanager v.1.0 allows a remote attacker to execute arbitrary code via the username parameter in the student list function.	5.4	More Details
CVE-2023-38911	A Cross-Site Scripting (XSS) vulnerability in CSZ CMS 1.3.0 allows attackers to execute arbitrary code via a crafted payload to the Gallery parameter in the YouTube URL fields.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20203	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid credentials to access the web-based management interface of the affected device.	5.4	More Details
CVE-2022-48538	In Cacti 1.2.19, there is an authentication bypass in the web login functionality because of improper validation in the PHP code: cacti_ldap_auth() allows a zero as the password.	5.3	More Details
CVE-2023-4040	The Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the eh_callback_handler function in versions up to, and including, 3.7.9. This makes it possible for unauthenticated attackers to modify the order status of arbitrary WooCommerce orders.	5.3	More Details
CVE-2023-39974	Exposure of Sensitive Information vulnerability in AcyMailing Enterprise component for Joomla. It allows unauthorized actors to get the number of subscribers in a specific list.	5.3	More Details
CVE-2023-40021	Oppia is an online learning platform. When comparing a received CSRF token against the expected token, Oppia uses the string equality operator (`==`), which is not safe against timing attacks. By repeatedly submitting invalid tokens, an attacker can brute-force the expected CSRF token character by character. Once they have recovered the token, they can then submit a forged request on behalf of a logged-in user and execute privileged actions on that user's behalf. In particular the function to validate received CSRF tokens is at `oppia.core.controllers.base.CsrfTokenManager.is_csrf_token_valid`. An attacker who can lure a logged-in Oppia user to a malicious website can perform any change on Oppia that the user is authorized to do, including changing profile information; creating, deleting, and changing explorations; etc. Note that the attacker cannot change a user's login credentials. An attack would need to complete within 1 second because every second, the time used in computing the token changes. This issue has been addressed in commit `b89bf80837` which has been included in release `3.3.2-hotfix-2`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40315	In OpenMNS Horizon 31.0.8 and versions earlier than 32.0.2 and related Meridian versions, any user that has the ROLE_FILESYSTEM_EDITOR can easily escalate their privileges to ROLE_ADMIN or any other role. 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-2023-40349	Jenkins Gogs Plugin 1.0.15 and earlier improperly initializes an option to secure its webhook endpoint, allowing unauthenticated attackers to trigger builds of jobs.	5.3	More Details
CVE-2023-35009	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could allow a remote attacker to obtain system information without authentication which could be used in reconnaissance to gather information that could be used for future attacks. IBM X-Force ID: 257703.	5.3	More Details
CVE-2023-32488	Dell PowerScale OneFS, 8.2.x-9.5.0.x, contains an information disclosure vulnerability in NFS. A low privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	5.3	More Details
CVE-2023-39743	lrzip-next LZMA v23.01 was discovered to contain an access violation via the component /bz3_decode_block src/libbz3.c.	5.3	More Details
CVE-2023-36674	An issue was discovered in MediaWiki before 1.35.11, 1.36.x through 1.38.x before 1.38.7, 1.39.x before 1.39.4, and 1.40.x before 1.40.1. It is possible to bypass the Bad image list (aka badFile) by using the thumb parameter (aka Manualthumb) of the File syntax.	5.3	More Details
CVE-2023-3244	The Comments Like Dislike plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the restore_settings function called via an AJAX action in versions up to, and including, 1.1.9. This makes it possible for authenticated attackers with minimal permissions, such as a subscriber, to reset the plugin's settings. NOTE: After attempting to contact the developer with no response, and reporting this to the WordPress plugin's team 30 days ago we are disclosing this issue as it still is not updated.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36844	A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to control certain, important environment variables. Using a crafted request an attacker is able to modify certain PHP environment variables leading to partial loss of integrity, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on EX Series: * All versions prior to 20.4R3-S9; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S7; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R3-S1; * 22.4 versions prior to 22.4R2-S2, 22.4R3; * 23.2 versions prior to 23.2R1-S1, 23.2R2.	5.3	More Details
CVE-2023-36846	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request to user.php that doesn't require authentication an attacker is able to upload arbitrary files via J-Web, leading to a loss of integrity for a certain part of the file system, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on SRX Series: * All versions prior to 20.4R3-S8; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2-S1, 22.4R3.	5.3	More Details
CVE-2023-20232	A vulnerability in the Tomcat implementation for Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to cause a web cache poisoning attack on an affected device. This vulnerability is due to improper input validation of HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a specific API endpoint on the Unified CCX Finesse Portal. A successful exploit could allow the attacker to cause the internal WebProxy to redirect users to an attacker-controlled host.	5.3	More Details
CVE-2023-40348	The webhook endpoint in Jenkins Gogs Plugin 1.0.15 and earlier provides unauthenticated attackers information about the existence of jobs in its output.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36847	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request to installAppPackage.php that doesn't require authentication an attacker is able to upload arbitrary files via J-Web, leading to a loss of integrity for a certain part of the file system, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on EX Series: * All versions prior to 20.4R3-S8; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S1; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2-S1, 22.4R3.	5.3	More Details
CVE-2023-32492	Dell PowerScale OneFS 9.5.0.x contains an incorrect default permissions vulnerability. A low-privileged local attacker could potentially exploit this vulnerability, leading to information disclosure or allowing to modify files.	5.3	More Details
CVE-2023-40251	Missing Encryption of Sensitive Data vulnerability in Genians Genian NAC V4.0, Genians Genian NAC V5.0, Genians Genian NAC Suite V5.0, Genians Genian ZTNA allows Man in the Middle Attack.This issue affects Genian NAC V4.0: from V4.0.0 through V4.0.155; Genian NAC V5.0: from V5.0.0 through V5.0.42 (Revision 117460); Genian NAC Suite V5.0: from V5.0.0 through V5.0.54; Genian ZTNA: from V6.0.0 through V6.0.15.	5.2	More Details
CVE-2023-24515	Server-Side Request Forgery (SSRF) vulnerability in API checker of Pandora FMS. Application does not have a check on the URL scheme used while retrieving API URL. Rather than validating the http/https scheme, the application allows other scheme such as file, which could allow a malicious user to fetch internal file content. This issue affects Pandora FMS v767 version and prior versions on all platforms.	5.2	More Details
CVE-2023-23565	An issue was discovered in Geomatika IsiGeo Web 6.0. It allows remote authenticated users to retrieve PHP files from the server via Local File Inclusion.	4.9	More Details
CVE-2023-2225	The SEO ALert WordPress plugin through 1.59 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-2254	The Ko-fi Button WordPress plugin before 1.3.3 does not properly some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup), and we consider it a low risk.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40281	EC-CUBE 2.11.0 to 2.17.2-p1 contain a cross-site scripting vulnerability in "mail/template" and "products/product" of Management page. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the other administrator or the user who accessed the website using the product.	4.8	More Details
CVE-2023-31942	Cross Site Scripting vulnerability found in Online Travel Agency System v.1.0 allows a remote attacker to execute arbitrary code via the description parameter in insert.php.	4.8	More Details
CVE-2023-20222	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details
CVE-2023-34412	A vulnerability in Red Lion Europe mbNET/mbNET.rokey and Helmholz REX 200 and REX 250 devices with firmware lower 7.3.2 allows an authenticated remote attacker with high privileges to inject malicious HTML or JavaScript code (XSS).	4.8	More Details
CVE-2023-20242	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details
CVE-2023-4422	Cross-site Scripting (XSS) - Stored in GitHub repository cockpit-hq/cockpit prior to 2.6.3.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3667	The Bit Assist WordPress plugin before 1.1.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-20201	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid credentials to access the web-based management interface of the affected device.	4.8	More Details
CVE-2023-25647	There is a permission and access control vulnerability in some ZTE mobile phones. Due to improper access control, applications in mobile phone could monitor the touch event.	4.7	More Details
CVE-2022-47022	An issue was discovered in open-mpi hwloc 2.1.0 allows attackers to cause a denial of service or other unspecified impacts via glibc-cpuset in topology-linux.c.	4.7	More Details
CVE-2023-32453	Dell BIOS contains an improper authentication vulnerability. A malicious user with physical access to the system may potentially exploit this vulnerability in order to modify a security-critical UEFI variable without knowledge of the BIOS administrator.	4.6	More Details
CVE-2020-21469	An issue was discovered in PostgreSQL 12.2 allows attackers to cause a denial of service via repeatedly sending SIGHUP signals. NOTE: this is disputed by the vendor because untrusted users cannot send SIGHUP signals; they can only be sent by a PostgreSQL superuser, a user with pg_reload_conf access, or a user with sufficient privileges at the OS level (the postgres account or the root account).	4.4	More Details
CVE-2020-27418	A Use After Free vulnerability in Fedora Linux kernel 5.9.0-rc9 allows attackers to obatin sensitive information via vgacon_invert_region() function.	4.4	More Details
CVE-2022-44730	Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache XML Graphics Batik.This issue affects Apache XML Graphics Batik: 1.16. A malicious SVG can probe user profile / data and send it directly as parameter to a URL.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2271	The Tiempo.com WordPress plugin through 0.1.2 does not have CSRF check when deleting its shortcode, which could allow attackers to make logged in admins delete arbitrary shortcode via a CSRF attack	4.3	More Details
CVE-2023-38732	IBM Robotic Process Automation 21.0.0 through 21.0.7 server could allow an authenticated user to view sensitive information from application logs. IBM X-Force ID: 262289.	4.3	More Details
CVE-2023-38733	IBM Robotic Process Automation 21.0.0 through 21.0.7.1 and 23.0.0 through 23.0.1 server could allow an authenticated user to view sensitive information from installation logs. IBM X-Force Id: 262293.	4.3	More Details
CVE-2023-3366	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.15.2 does not have CRSF check when deleting a shipment, allowing attackers to make any logged in user, delete arbitrary shipment via a CSRF attack	4.3	More Details
CVE-2023-4439	A vulnerability was found in SourceCodester Card Holder Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the component Minus Value Handler. The manipulation leads to improper validation of specified quantity in input. The attack may be launched remotely. The identifier of this vulnerability is VDB-237560.	4.3	More Details
CVE-2023-4303	Jenkins Fortify Plugin 22.1.38 and earlier does not escape the error message for a form validation method, resulting in an HTML injection vulnerability.	4.3	More Details
CVE-2023-4374	The WP Remote Users Sync plugin for WordPress is vulnerable to unauthorized access of data and addition of data due to a missing capability check on the 'refresh_logs_async' functions in versions up to, and including, 1.2.11. This makes it possible for authenticated attackers with subscriber privileges or above, to view logs.	4.3	More Details
CVE-2023-39973	Improper Access Control vulnerability in AcyMailing Enterprise component for Joomla. It allows the unauthorized removal of attachments from campaigns.	4.3	More Details
CVE-2023-39972	Improper Access Control vulnerability in AcyMailing Enterprise component for Joomla. It allows unauthorized users to create new mailing lists.	4.3	More Details
CVE-2023-4381	Unverified Password Change in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40351	A cross-site request forgery (CSRF) vulnerability in Jenkins Favorite View Plugin 5.v77a_37f62782d and earlier allows attackers to add or remove views from another user's favorite views tab bar.	4.3	More Details
CVE-2023-40337	A cross-site request forgery (CSRF) vulnerability in Jenkins Folders Plugin 6.846.v23698686f0f6 and earlier allows attackers to copy a view inside a folder.	4.3	More Details
CVE-2023-40338	Jenkins Folders Plugin 6.846.v23698686f0f6 and earlier displays an error message that includes an absolute path of a log file when attempting to access the Scan Organization Folder Log if no logs are available, exposing information about the Jenkins controller file system.	4.3	More Details
CVE-2023-20237	A vulnerability in Cisco Intersight Virtual Appliance could allow an unauthenticated, adjacent attacker to access internal HTTP services that are otherwise inaccessible. This vulnerability is due to insufficient restrictions on internally accessible http proxies. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker access to internal subnets beyond the sphere of their intended access level.	4.3	More Details
CVE-2023-40344	A missing permission check in Jenkins Delphix Plugin 3.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2023-4302	A missing permission check in Jenkins Fortify Plugin 22.1.38 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.2	More Details
CVE-2023-4301	A cross-site request forgery (CSRF) vulnerability in Jenkins Fortify Plugin 22.1.38 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.2	More Details
CVE-2023-40370	IBM Robotic Process Automation 21.0.0 through 21.0.7.1 runtime is vulnerable to information disclosure of script content if the remote REST request computer policy is enabled. IBM X-Force ID: 263470.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4384	A vulnerability has been found in MaximaTech Portal Executivo 21.9.1.140 and classified as problematic. This vulnerability affects unknown code of the component Cookie Handler. The manipulation leads to missing encryption of sensitive data. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-237316. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2023-4392	A vulnerability was found in Control iD Gerencia Web 1.30 and classified as problematic. Affected by this issue is some unknown functionality of the component Cookie Handler. The manipulation leads to cleartext storage of sensitive information. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-237380. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2023-4382	A vulnerability, which was classified as problematic, has been found in tdevs Hyip Rio 2.1. Affected by this issue is some unknown functionality of the file /user/settings of the component Profile Settings. The manipulation of the argument avatar leads to cross site scripting. The attack may be launched remotely. VDB-237314 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-2023-39061	Cross Site Request Forgery (CSRF) vulnerability in Chamilo v.1.11 thru v.1.11.20 allows a remote authenticated privileged attacker to execute arbitrary code.	3.5	More Details
CVE-2020-19909	Integer overflow vulnerability in tool_operate.c in curl 7.65.2 via a large value as the retry delay. NOTE: many parties report that this has no direct security impact on the curl user; however, it may (in theory) cause a denial of service to associated systems or networks if, for example, --retry-delay is misinterpreted as a value much smaller than what was intended. This is not especially plausible because the overflow only happens if the user was trying to specify that curl should wait weeks (or longer) before trying to recover from a transient error.	3.3	More Details
CVE-2023-38158	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-14834. Reason: This candidate is a reservation duplicate of CVE-2019-14834. Notes: All CVE users should reference CVE-2019-14834 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2020-19500	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4367	Rejected reason: Duplicate, use CVE-2023-4279 instead.	N/A	More Details
CVE-2023-30078	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-32181. Reason: This record is a duplicate of CVE-2023-32181. Notes: All CVE users should reference CVE-2023-32181 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-40433	Rejected reason: ** REJECT ** This CVE ID has been rejected by its CNA as it was not a security issue.	N/A	More Details
CVE-2023-4413	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: Permission to access the file is limited to administrative users only by default.	N/A	More Details
CVE-2023-30079	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-22652. Reason: This record is a duplicate of CVE-2023-22652. Notes: All CVE users should reference CVE-2023-22652 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details