SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 May 2023

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-2024	Improper authentication in OpenBlue Enterprise Manager Data Collector versions prior to 3.2.5.75 allow access to an unauthorized user under certain circumstances.	10.0	More Details
CVE-2023-31098	Weak Password Requirements vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.6.0. When users change their password to a simple password (with any character or symbol), attackers can easily guess the user's password and access the account. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7805 https://github.com/apache/inlong/pull/7805 to solve it.	9.8	More Details
CVE-2023-28413	Directory traversal vulnerability in Snow Monkey Forms versions v5.0.6 and earlier allows a remote unauthenticated attacker to obtain sensitive information, alter the website, or cause a denial-of-service (DoS) condition.	9.8	More Details
CVE-2023-31689	In Wcms 0.3.2, an attacker can send a crafted request from a vulnerable web application backend server /wcms/wex/html.php via the finish parameter and the textAreaCode parameter. It can write arbitrary strings into custom file names and upload any files, and write malicious code to execute scripts to trigger command execution.	9.8	More Details
CVE-2020-20012	WebPlus Pro v1.4.7.8.4-01 is vulnerable to Incorrect Access Control.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27068	Deserialization of Untrusted Data in Sitecore Experience Platform through 10.2 allows remote attackers to run arbitrary code via ValidationResult.aspx.	9.8	More Details
CVE-2023-31814	D-Link DIR-300 firmware <=REVA1.06 and <=REVB2.06 is vulnerable to File inclusion via /model/__lang_msg.php.	9.8	More Details
CVE-2023-25953	Code injection vulnerability in Drive Explorer for macOS versions 3.5.4 and earlier allows an attacker who can login to the client where the affected product is installed to inject arbitrary code while processing the product execution. Since a full disk access privilege is required to execute LINE WORKS Drive Explorer, the attacker may be able to read and/or write to arbitrary files without the access privileges.	9.8	More Details
CVE-2023-27388	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	9.8	More Details
CVE-2023-27397	Unrestricted upload of file with dangerous type exists in MicroEngine Mailform version 1.1.0 to 1.1.8. If the product's file upload function and server save option are enabled, a remote attacker may save an arbitrary file on the server and execute it.	9.8	More Details
CVE-2023-27507	MicroEngine Mailform version 1.1.0 to 1.1.8 contains a path traversal vulnerability. If the product's file upload function and server save option are enabled, a remote attacker may save an arbitrary file on the server and execute it.	9.8	More Details
CVE-2023-28408	Directory traversal vulnerability in MW WP Form versions v4.4.2 and earlier allows a remote unauthenticated attacker to alter the website or cause a denial-of-service (DoS) condition, and obtain sensitive information depending on settings.	9.8	More Details
CVE-2023-28409	Unrestricted upload of file with dangerous type exists in MW WP Form versions v4.4.2 and earlier, which may allow a remote unauthenticated attacker to upload an arbitrary file.	9.8	More Details
CVE-2023-33338	Old Age Home Management 1.0 is vulnerable to SQL Injection via the username parameter.	9.8	More Details
CVE-2023-33294	An issue was discovered in KaiOS 3.0 before 3.1. The /system/bin/tctweb_server binary exposes a local web server that responds to GET and POST requests on port 2929. The server accepts arbitrary Bash commands and executes them as root. Because it is not permission or context restricted and returns proper CORS headers, it's accessible to all websites via the browser. At a bare minimum, this allows an attacker to retrieve a list of the user's installed apps, notifications, and downloads. It also allows an attacker to delete local files and modify system properties including the boolean persist.moz.killswitch property (which would render the device inoperable). This vulnerability is partially mitigated by SELinux which prevents reads, writes, or modifications to files or permissions within protected partitions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33361	Piwigo 13.6.0 is vulnerable to SQL Injection via /admin/permalinks.php.	9.8	More Details
CVE-2023-33362	Piwigo 13.6.0 is vulnerable to SQL Injection via in the "profile" function.	9.8	More Details
CVE-2023-23298	The `Toybox.Graphics.BufferedBitmap.initialize` API method in CIQ API version 2.3.0 through 4.1.7 does not validate its parameters, which can result in integer overflows when allocating the underlying bitmap buffer. A malicious application could call the API method with specially crafted parameters and hijack the execution of the device's firmware.	9.8	More Details
CVE-2023-23300	The `Toybox.Cryptography.Cipher.initialize` API method in CIQ API version 3.0.0 through 4.1.7 does not validate its parameters, which can result in buffer overflows when copying data. A malicious application could call the API method with specially crafted parameters and hijack the execution of the device's firmware.	9.8	More Details
CVE-2023-23301	The `news` MonkeyC operation code in CIQ API version 1.0.0 through 4.1.7 fails to check that string resources are not extending past the end of the expected sections. A malicious CIQ application could craft a string that starts near the end of a section, and whose length extends past its end. Upon loading the string, the GarminOS TVM component may read out-of-bounds memory.	9.8	More Details
CVE-2023-23302	The `Toybox.GenericChannel.setDeviceConfig` API method in CIQ API version 1.2.0 through 4.1.7 does not validate its parameter, which can result in buffer overflows when copying various attributes. A malicious application could call the API method with specially crafted object and hijack the execution of the device's firmware.	9.8	More Details
CVE-2023-23303	The `Toybox.Ant.GenericChannel.enableEncryption` API method in CIQ API version 3.2.0 through 4.1.7 does not validate its parameter, which can result in buffer overflows when copying various attributes. A malicious application could call the API method with specially crafted object and hijack the execution of the device's firmware.	9.8	More Details
CVE-2023-23305	The GarminOS TVM component in CIQ API version 1.0.0 through 4.1.7 is vulnerable to various buffer overflows when loading binary resources. A malicious application embedding specially crafted resources could hijack the execution of the device's firmware.	9.8	More Details
CVE-2023-23306	The `Toybox.Ant.BurstPayload.add` API method in CIQ API version 2.2.0 through 4.1.7 suffers from a type confusion vulnreability, which can result in an out-of-bounds write operation. A malicious application could create a specially crafted `Toybox.Ant.BurstPayload` object, call its `add` method, override arbitrary memory and hijack the execution of the device's firmware.	9.8	More Details
CVE-2023-31752	SourceCodester Employee and Visitor Gate Pass Logging System v1.0 is vulnerable to SQL Injection via /employee_gatepass/classes/Login.php.	9.8	More Details
CVE-2023-2840	NULL Pointer Dereference in GitHub repository gpac/gpac prior to 2.2.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1508	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Adam Retail Automation Systems Mobilmen Terminal Software allows SQL Injection.This issue affects Mobilmen Terminal Software: before 3.	9.8	More Details
CVE-2023-28081	A bytecode optimization bug in Hermes prior to commit e6ed9c1a4b02dc219de1648f44cd808a56171b81 could be used to cause an use-after-free and obtain arbitrary code execution via a carefully crafted payload. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2023-29985	Sourcecodester Student Study Center Desk Management System v1.0 admin\reports\index.php#date_from has a SQL Injection vulnerability.	9.8	More Details
CVE-2023-27217	A stack-based buffer overflow in the ChangeFriendlyName() function of Belkin Smart Outlet V2 F7c063 firmware_2.00.11420.OWRT.PVT_SNSV2 allows attackers to cause a Denial of Service (DoS) via a crafted UPNP request.	9.8	More Details
CVE-2023-30333	An arbitrary file upload vulnerability in the component /admin/ThemeController.java of PerfreeBlog v3.1.2 allows attackers to execute arbitrary code via a crafted file.	9.8	More Details
CVE-2023-23556	An error in BigInt conversion to Number in Hermes prior to commit a6dcafe6ded8e61658b40f5699878cd19a481f80 could have been used by a malicious attacker to execute arbitrary code due to an out-of-bound write. Note that this bug is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2023-23557	An error in Hermes' algorithm for copying objects properties prior to commit a00d237346894c6067a594983be6634f4168c9ad could be used by a malicious attacker to execute arbitrary code via type confusion. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2023-25933	A type confusion bug in TypedArray prior to commit e6ed9c1a4b02dc219de1648f44cd808a56171b81 could have been used by a malicious attacker to execute arbitrary code via untrusted JavaScript. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2023-2319	It was discovered that an update for PCS package in RHBA-2023:2151 erratum released as part of Red Hat Enterprise Linux 9.2 failed to include the fix for the Webpack issue CVE-2023-28154 (for PCS package), which was previously addressed in Red Hat Enterprise Linux 9.1 via erratum RHSA-2023:1591. The CVE-2023-2319 was assigned to that Red Hat specific security regression in Red Hat Enterprise Linux 9.2.	9.8	More Details
CVE-2023-28753	netconsd prior to v0.2 was vulnerable to an integer overflow in its parse_packet function. A malicious individual could leverage this overflow to create heap memory corruption with attacker controlled data.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30470	A use-after-free related to unsound inference in the bytecode generation when optimizations are enabled for Hermes prior to commit da8990f737ebb9d9810633502f65ed462b819c09 could have been used by an attacker to achieve remote code execution. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	9.8	More Details
CVE-2023-2704	The BP Social Connect plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.5. This is due to insufficient verification on the user being supplied during a Facebook login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	9.8	More Details
CVE-2023-31707	SEMCMS 1.5 is vulnerable to SQL Injection via Ant_Rponse.php.	9.8	More Details
CVE-2023-2276	The WCFM Membership – WooCommerce Memberships for Multivendor Marketplace plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 2.10.7. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts.	9.8	More Details
CVE-2023-2712	Unrestricted Upload of File with Dangerous Type vulnerability in "Rental Module" developed by third-party for Ideasoft's E-commerce Platform allows Command Injection, Using Malicious Files, Upload a Web Shell to a Web Server.This issue affects Rental Module: before 23.05.15.	9.8	More Details
CVE-2023-2780	Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.3.1.	9.8	More Details
CVE-2023-2713	Authorization Bypass Through User-Controlled Key vulnerability in "Rental Module" developed by third-party for Ideasoft's E-commerce Platform allows Authentication Abuse, Authentication Bypass.This issue affects Rental Module: before 23.05.15.	9.8	More Details
CVE-2023-33236	MXsecurity version 1.0 is vulnearble to hardcoded credential vulnerability. This vulnerability has been reported that can be exploited to craft arbitrary JWT tokens and subsequently bypass authentication for web-based APIs.	9.8	More Details
CVE-2023-30191	PrestaShop cdesigner < 3.1.9 is vulnerable to SQL Injection via CdesignerTraitementModuleFrontController::initContent().	9.8	More Details
CVE-2023-31062	Improper Privilege Management Vulnerabilities in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. When the attacker has access to a valid (but unprivileged) account, the exploit can be executed using Burp Suite by sending a login request and following it with a subsequent HTTP request using the returned cookie. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31903	GuppY CMS 6.00.10 is vulnerable to Unrestricted File Upload which allows remote attackers to execute arbitrary code by uploading a php file.	9.8	More Details
CVE-2023-31902	RPA Technology Mobile Mouse 3.6.0.4 is vulnerable to Remote Code Execution (RCE).	9.8	More Details
CVE-2023-31729	TOTOLINK A3300R v17.0.0cu.557 is vulnerable to Command Injection via /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2023-30438	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706.	9.3	More Details
CVE-2023-29919	SolarView Compact <= 6.0 is vulnerable to Insecure Permissions. Any file on the server can be read or modified because texteditor.php is not restricted.	9.1	More Details
CVE-2023-23304	The GarminOS TVM component in CIQ API version 2.1.0 through 4.1.7 allows applications with a specially crafted head section to use the `Toybox.SensorHistory` module without permission. A malicious application could call any functions from the `Toybox.SensorHistory` module without the user's consent and disclose potentially private or sensitive information.	9.1	More Details
CVE-2023-2838	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.2.2.	9.1	More Details
CVE-2023-31065	Insufficient Session Expiration vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. An old session can be used by an attacker even after the user has been deleted or the password has been changed. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 , https://github.com/apache/inlong/pull/7884 https://github.com/apache/inlong/pull/7884 to solve it.	9.1	More Details
CVE-2023-31066	Files or Directories Accessible to External Parties vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Different users in InLong could delete, edit, stop, and start others' sources! Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7775 https://github.com/apache/inlong/pull/7775 to solve it.	9.1	More Details
CVE-2023-31703	Cross Site Scripting (XSS) in the edit user form in Microworld Technologies eScan management console 14.0.1400.2281 allows remote attacker to inject arbitrary code via the from parameter.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2586	Teltonika’s Remote Management System versions 4.14.0 is vulnerable to an unauthorized attacker registering previously unregistered devices through the RMS platform. If the user has not disabled the "RMS management feature" enabled by default, then an attacker could register that device to themselves. This could enable the attacker to perform different operations on the user's devices, including remote code execution with 'root' privileges (using the 'Task Manager' feature on RMS).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-32697	SQLite JDBC is a library for accessing and creating SQLite database files in Java. Sqlite-jdbc addresses a remote code execution vulnerability via JDBC URL. This issue impacting versions 3.6.14.1 through 3.41.2.1 and has been fixed in version 3.41.2.2.	8.8	More Details
CVE-2023-27521	OS command injection vulnerability in the mail setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows remote authenticated attackers to execute an arbitrary OS command.	8.8	More Details
CVE-2023-2588	Teltonika’s Remote Management System versions prior to 4.10.0 have a feature allowing users to access managed devices’ local secure shell (SSH)/web management services over the cloud proxy. A user can request a web proxy and obtain a URL in the Remote Management System cloud subdomain. This URL could be shared with others without Remote Management System authentication . An attacker could exploit this vulnerability to create a malicious webpage that uses a trusted and certified domain. An attacker could initiate a reverse shell when a victim connects to the malicious webpage, achieving remote code execution on the victim device.	8.8	More Details
CVE-2023-27233	Piwigo before 13.6.0 was discovered to contain a SQL injection vulnerability via the order[0][dir] parameter at user_list_backend.php.	8.8	More Details
CVE-2023-31923	Suprema BioStar 2 before 2022 Q4, v2.9.1 has Insecure Permissions. A vulnerability in the web application allows an authenticated attacker with "User Operator" privileges to create a highly privileged user account. The vulnerability is caused by missing server-side validation, which can be exploited to gain full administrator privileges on the system.	8.8	More Details
CVE-2022-46680	A CWE-319: Cleartext transmission of sensitive information vulnerability exists that could cause disclosure of sensitive information, denial of service, or modification of data if an attacker is able to intercept network traffic.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24805	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. If you use the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >> 8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with network access to the hosted print server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to network printers in the meantime.	8.8	More Details
CVE-2023-32336	IBM InfoSphere Information Server 11.7 is affected by a remote code execution vulnerability due to insecure deserialization in an RMI service. IBM X-Force ID: 255285.	8.8	More Details
CVE-2023-31701	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceRemove.	8.8	More Details
CVE-2023-31700	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceAdd.	8.8	More Details
CVE-2023-31996	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	8.8	More Details
CVE-2023-25946	Authentication bypass vulnerability in Qrio Lock (Q-SL2) firmware version 2.0.9 and earlier allows a network-adjacent attacker to analyze the product's communication data and conduct an arbitrary operation under certain conditions.	8.8	More Details
CVE-2023-27387	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	8.8	More Details
CVE-2023-27514	OS command injection vulnerability in the download page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute an arbitrary OS command.	8.8	More Details
CVE-2023-27518	Buffer overflow vulnerability in the multiple setting pages of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute arbitrary code.	8.8	More Details
CVE-2023-2203	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28394	Beekeeper Studio versions prior to 3.9.9 allows a remote authenticated attacker to execute arbitrary JavaScript code with the privilege of the application on the PC where the affected product is installed. As a result, an arbitrary OS command may be executed as well.	8.8	More Details
CVE-2023-0863	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5.	8.8	More Details
CVE-2023-31848	davinci 0.3.0-rc is vulnerable to Server-side request forgery (SSRF).	8.8	More Details
CVE-2023-2702	Authorization Bypass Through User-Controlled Key vulnerability in Finex Media Competition Management System allows Authentication Abuse, Authentication Bypass.This issue affects Competition Management System: before 23.07.	8.8	More Details
CVE-2023-20159	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-31241	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright.	8.6	More Details
CVE-2023-20158	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-20024	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-28649	The Hub in the Snap One OvrC cloud platform is a device used to centralize and manage nested devices connected to it. A vulnerability exists in which an attacker could impersonate a hub and send device requests to claim already claimed devices. The OvrC cloud platform receives the requests but does not validate if the found devices are already managed by another user.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20161	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-20160	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-28386	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution.	8.6	More Details
CVE-2023-20156	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-20157	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-20162	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2023-20189	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	8.6	More Details
CVE-2022-47311	A proprietary protocol for iBoot devices is used for control and keepalive commands. The function compares the username and password; it also contains the configuration data for the user specified. If the user does not exist, then it sends a value for username and password, which allows successful authentication for a connection.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1837	Missing Authentication for critical function vulnerability in HYPR Server allows Authentication Bypass when using Legacy APIs.This issue affects HYPR Server: before 8.0 (with enabled Legacy APIs)	8.5	More Details
CVE-2023-2504	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded credentials.	8.4	More Details
CVE-2023-25183	In Snap One OvrC Pro versions prior to 7.2, when logged into the superuser account, a new functionality appears that could allow users to execute arbitrary commands on the hub device.	8.3	More Details
CVE-2023-31240	Snap One OvrC Pro versions prior to 7.2 have their own locally running web server accessible both from the local network and remotely. OvrC cloud contains a hidden superuser account accessible through hard-coded credentials.	8.3	More Details
CVE-2023-31208	Improper neutralization of livestatus command delimiters in the RestAPI in Checkmk < 2.0.0p36, < 2.1.0p28, and < 2.2.0b8 (beta) allows arbitrary livestatus command execution for authorized users.	8.3	More Details
CVE-2023-33244	Obsidian before 1.2.2 allows calls to unintended APIs (for microphone access, camera access, and desktop notification) via an embedded web page.	8.2	More Details
CVE-2023-20881	Cloud foundry instances having CAPI version between 1.140 and 1.152.0 along with loggregator-agent v7+ may override other users syslog drain credentials if they're aware of the client certificate used for that syslog drain. This applies even if the drain has zero certs. This would allow the user to override the private key and add or modify a certificate authority used for the connection.	8.1	More Details
CVE-2023-32347	Teltonika’s Remote Management System versions prior to 4.10.0 use device serial numbers and MAC addresses to identify devices from the user perspective for device claiming and from the device perspective for authentication. If an attacker obtained the serial number and MAC address of a device, they could authenticate as that device and steal communication credentials of the device. This could allow an attacker to enable arbitrary command execution as root by utilizing management options within the newly registered devices.	8.1	More Details
CVE-2023-2706	The OTP Login Woocommerce & Gravity Forms plugin for WordPress is vulnerable to authentication bypass. This is due to the fact that when generating OTP codes for users to use in order to login via phone number, the plugin returns these codes in an AJAX response. This makes it possible for unauthenticated attackers to obtain login codes for administrators. This does require an attacker have access to the phone number configured for an account, which can be obtained via social engineering or reconnaissance.	8.1	More Details
CVE-2023-2845	Improper Access Control in GitHub repository cloudexplorer-dev/cloudexplorer-lite prior to v1.1.0.	8.1	More Details
CVE-2022-47320	The iBoot device’s basic discovery protocol assists in initial device configuration. The discovery protocol shows basic information about devices on the network and allows users to perform configuration changes.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32350	Versions 00.07.00 through 00.07.03 of Teltonika's RUT router firmware contain an operating system (OS) command injection vulnerability in a Lua service. An attacker could exploit a parameter in the vulnerable function that calls a user-provided package name by instead providing a package with a malicious name that contains an OS command injection payload.	8.0	More Details
CVE-2023-32349	Version 00.07.03.4 and prior of Teltonika's RUT router firmware contain a packet dump utility that contains proper validation for filter parameters. However, variables for validation checks are stored in an external configuration file. An authenticated attacker could use an exposed UCI configuration utility to change these variables and enable malicious parameters in the dump utility, which could result in arbitrary code execution.	8.0	More Details
CVE-2022-0010	Insertion of Sensitive Information into Log File vulnerability in ABB QCS 800xA, ABB QCS AC450, ABB Platform Engineering Tools. An attacker, who already has local access to the QCS nodes, could successfully obtain the password for a system user account. Using this information, the attacker could have the potential to exploit this vulnerability to gain control of system nodes. This issue affects QCS 800xA: from 1.0;0 through 6.1SP2; QCS AC450: from 1.0;0 through 5.1SP2; Platform Engineering Tools: from 1.0:0 through 2.3.0.	7.8	More Details
CVE-2023-33240	Foxit PDF Reader (12.1.1.15289 and earlier) and Foxit PDF Editor (12.1.1.15289 and all previous 12.x versions, 11.2.5.53785 and all previous 11.x versions, and 10.1.11.37866 and earlier) on Windows allows Local Privilege Escalation when installed to a non-default directory because unprivileged users have access to an executable file of a system service. This is fixed in 12.1.2.	7.8	More Details
CVE-2023-2491	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2.	7.8	More Details
CVE-2023-33204	sysstat through 12.7.2 allows a multiplication integer overflow in check_overflow in common.c. NOTE: this issue exists because of an incomplete fix for CVE-2022-39377.	7.8	More Details
CVE-2023-32700	LuaTeX before 1.17.0 allows execution of arbitrary shell commands when compiling a TeX file obtained from an untrusted source. This occurs because luatex-core.lua lets the original io.popen be accessed. This also affects TeX Live before 2023 r66984 and MiKTeX before 23.5.	7.8	More Details
CVE-2023-31747	Wondershare Filmora 12 (Build 12.2.1.2088) was discovered to contain an unquoted service path vulnerability via the component NativePushService. This vulnerability allows attackers to launch processes with elevated privileges.	7.8	More Details
CVE-2022-45452	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Agent (Windows) before build 30430, Acronis Cyber Protect 15 (Windows) before build 30984.	7.8	More Details
CVE-2022-4418	Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40208.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29838	Insecure Permission vulnerability found in Botkind/Siber Systems SyncApp v.19.0.3.0 allows a local attacker toe escalate privileges via the SyncService.exe file.	7.8	More Details
CVE-2023-31871	OpenText Documentum Content Server before 23.2 has a flaw that allows for privilege escalation from a non-privileged Documentum user to root. The software comes prepackaged with a root owned SUID binary dm_secure_writer. The binary has security controls in place preventing creation of a file in a non-owned directory, or as the root user. However, these controls can be carefully bypassed to allow for an arbitrary file write as root.	7.8	More Details
CVE-2023-31724	yasm 1.3.0.55.g101bc was discovered to contain a segmentation violation via the function do_directive at /nasm/nasm-pp.c.	7.8	More Details
CVE-2023-31826	Skyscreamer Open Source Nevado JMS v1.3.2 does not perform security checks when receiving messages. This allows attackers to execute arbitrary commands via supplying crafted data.	7.8	More Details
CVE-2023-31722	There exists a heap buffer overflow in nasm 2.16.02rc1 (GitHub commit: b952891).	7.8	More Details
CVE-2023-2505	The affected products have a CSRF vulnerability that could allow an attacker to execute code and upload malicious files.	7.7	More Details
CVE-2023-30469	Cross-site Scripting vulnerability in Hitachi Ops Center Analyzer (Hitachi Ops Center Analyzer detail view component) allows Reflected XSS.This issue affects Hitachi Ops Center Analyzer: from 10.9.1-00 before 10.9.2-00.	7.6	More Details
CVE-2023-31655	redis v7.0.10 was discovered to contain a segmentation violation. This vulnerability allows attackers to cause a Denial of Service (DoS) via unspecified vectors.	7.5	More Details
CVE-2022-45459	Sensitive information disclosure due to insecure registry permissions. The following products are affected: Acronis Agent (Windows) before build 30025, Acronis Cyber Protect 15 (Windows) before build 30984.	7.5	More Details
CVE-2023-1618	Active Debug Code vulnerability in Mitsubishi Electric Corporation MELSEC WS Series WS0-GETH00200 Serial number 2310 **** and prior allows a remote unauthenticated attacker to bypass authentication and illegally log into the affected module by connecting to it via telnet which is hidden function and is enabled by default when shipped from the factory. As a result, a remote attacker with unauthorized login can reset the module, and if certain conditions are met, he/she can disclose or tamper with the module's configuration or rewrite the firmware.	7.5	More Details
CVE-2023-1694	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24833	A use-after-free in BigIntPrimitive addition in Hermes prior to commit a6dcafe6ded8e61658b40f5699878cd19a481f80 could have been used by an attacker to leak raw data from Hermes VM's heap. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	7.5	More Details
CVE-2023-1692	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-1696	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-30199	Prestashop customexporter <= 1.7.20 is vulnerable to Incorrect Access Control via modules/customexporter/downloads/download.php.	7.5	More Details
CVE-2022-30114	A heap-based buffer overflow in a network service in Fastweb FASTGate MediaAccess FGA2130FWB, firmware version 18.3.n.0482_FW_230_FGA2130, and DGA4131FWB, firmware version up to 18.3.n.0462_FW_261_DGA4131, allows a remote attacker to reboot the device through a crafted HTTP request, causing DoS.	7.5	More Details
CVE-2023-23759	There is a vulnerability in the fizz library prior to v2023.01.30.00 where a CHECK failure can be triggered remotely. This behavior requires the client supported cipher advertisement changing between the original ClientHello and the second ClientHello, crashing the process (impact is limited to denial of service).	7.5	More Details
CVE-2023-24832	A null pointer dereference bug in Hermes prior to commit 5cae9f72975cf0e5a62b27fdd8b01f103e198708 could have been used by an attacker to crash an Hermes runtime where the EnableHermesInternal config option was set to true. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected.	7.5	More Details
CVE-2023-1693	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-31064	Files or Directories Accessible to External Parties vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. the user in InLong could cancel an application that doesn't belongs to it. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7799 https://github.com/apache/inlong/pull/7799 to solve it.	7.5	More Details
CVE-2023-33252	iden3 snarkjs through 0.6.11 allows double spending because there is no validation that the publicSignals length is less than the field modulus.	7.5	More Details
CVE-2023-2839	Divide By Zero in GitHub repository gpac/gpac prior to 2.2.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31726	AList 3.15.1 is vulnerable to Incorrect Access Control, which can be exploited by attackers to obtain sensitive information.	7.5	More Details
CVE-2023-31517	A memory leak in the component CConsole::Chain of Teeworlds v0.7.5 allows attackers to cause a Denial of Service (DoS) via opening a crafted file.	7.5	More Details
CVE-2023-2703	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Finex Media Competition Management System allows Retrieve Embedded Sensitive Data, Collect Data as Provided by Users.This issue affects Competition Management System: before 23.07.	7.5	More Details
CVE-2023-23299	The permission system implemented and enforced by the GarminOS TVM component in CIQ API version 1.0.0 through 4.1.7 can be bypassed entirely. A malicious application with specially crafted code and data sections could access restricted CIQ modules, call their functions and disclose sensitive data such as user profile information and GPS coordinates, among others.	7.5	More Details
CVE-2023-31670	An issue in wasm2c 1.0.32, wasm2wat 1.0.32, wasm-decompile 1.0.32, and wasm-validate 1.0.32 allows attackers to cause a Denial of Service (DoS) via running a crafted binary.	7.5	More Details
CVE-2023-31193	Snap One OvrC Pro versions prior to 7.3 use HTTP connections when downloading a program from their servers. Because they do not use HTTPS, OvrC Pro devices are susceptible to exploitation.	7.5	More Details
CVE-2023-27067	Directory Traversal vulnerability in Sitecore Experience Platform through 10.2 allows remote attackers to download arbitrary files via crafted command to download.aspx	7.5	More Details
CVE-2023-31103	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers can change the immutable name and type of cluster of InLong. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891 to solve it.	7.5	More Details
CVE-2023-33297	Bitcoin Core before 24.1, when debug mode is not used, allows attackers to cause a denial of service (e.g., CPU consumption) because draining the inventory-to-send queue is inefficient, as exploited in the wild in May 2023.	7.5	More Details
CVE-2022-45457	Sensitive information disclosure and manipulation due to improper certification validation. The following products are affected: Acronis Agent (Windows) before build 29633, Acronis Cyber Protect 15 (Windows) before build 30984.	7.5	More Details
CVE-2023-2587	Teltonika’s Remote Management System versions prior to 4.10.0 contain a cross-site scripting (XSS) vulnerability in the main page of the web interface. An attacker with the MAC address and serial number of a connected device could send a maliciously crafted JSON file with an HTML object to trigger the vulnerability. This could allow the attacker to execute scripts in the account context and obtain remote code execution on managed devices.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31454	Incorrect Permission Assignment for Critical Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. The attacker can bind any cluster, even if he is not the cluster owner. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it.[1] https://github.com/apache/inlong/pull/7947 https://github.com/apache/inlong/pull/7947	7.5	More Details
CVE-2023-31453	Incorrect Permission Assignment for Critical Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. The attacker can delete others' subscriptions, even if they are not the owner of the deleted subscription. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/7949 https://github.com/apache/inlong/pull/7949	7.5	More Details
CVE-2023-31206	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers can change the immutable name and type of nodes of InLong. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it. [1] https://cveprocess.apache.org/cve5/[1]%C2%A0https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891	7.5	More Details
CVE-2023-31058	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers would bypass the 'autoDeserialize' option filtering by adding blanks. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7674 https://github.com/apache/inlong/pull/7674 to solve it.	7.5	More Details
CVE-2023-28709	The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur.	7.5	More Details
CVE-2022-45458	Sensitive information disclosure and manipulation due to improper certification validation. The following products are affected: Acronis Agent (Windows, macOS, Linux) before build 29633, Acronis Cyber Protect 15 (Windows, macOS, Linux) before build 30984.	7.5	More Details
CVE-2023-2736	The Groundhogg plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.7.9.8. This is due to missing nonce validation in the 'ajax_edit_contact' function. This makes it possible for authenticated attackers to receive the auto login link via shortcode and then modify the assigned user to the auto login link to elevate verified user privileges via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	7.5	More Details
CVE-2022-45453	TLS/SSL weak cipher suites enabled. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 30984.	7.5	More Details
CVE-2023-32767	The web interface of Symcon IP-Symcon before 6.3 (i.e., before 2023-05-12) allows a remote attacker to read sensitive files via .. directory-traversal sequences in the URL.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45450	Sensitive information disclosure and manipulation due to improper authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 28610, Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 30984.	7.5	More Details
CVE-2023-2295	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2.	7.5	More Details
CVE-2023-31904	savysoda Wifi HD Wireless Disk Drive 11 is vulnerable to Local File Inclusion.	7.5	More Details
CVE-2023-2757	The Waiting: One-click countdowns plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on 'saveLang' functions in versions up to, and including, 0.6.2. This could lead to Cross-Site Scripting due to insufficient input sanitization and output escaping. This makes it possible for subscriber-level attackers to access functions to save plugin data that can potentially lead to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.4	More Details
CVE-2023-30382	A buffer overflow in the component hl.exe of Valve Half-Life up to 5433873 allows attackers to execute arbitrary code and escalate privileges by supplying crafted parameters.	7.3	More Details
CVE-2019-25137	Umbraco CMS 4.11.8 through 7.15.10, and 7.12.4, allows Remote Code Execution by authenticated administrators via msxsl:script in an xsltSelection to developer/Xslt/xsltVisualize.aspx.	7.2	More Details
CVE-2023-32679	Craft CMS is an open source content management system. In affected versions of Craft CMS an unrestricted file extension may lead to Remote Code Execution. If the name parameter value is not empty string('') in the View.php's doesTemplateExist() -> resolveTemplate() -> _resolveTemplateInternal() -> _resolveTemplate() function, it returns directly without extension verification, so that arbitrary extension files are rendered as twig templates. When attacker with admin privileges on a DEV or an improperly configured STG or PROD environment, they can exploit this vulnerability to remote code execution. Code execution may grant the attacker access to the host operating system. This issue has been addressed in version 4.4.6. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details
CVE-2023-33235	MXsecurity version 1.0 is vulnearble to command injection vulnerability. This vulnerability has been reported in the SSH CLI program, which can be exploited by attackers who have gained authorization privileges. The attackers can break out of the restricted shell and subsequently execute arbitrary code.	7.2	More Details
CVE-2023-2832	SQL Injection in GitHub repository unilogies/bumsys prior to 2.2.0.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33617	An OS Command Injection vulnerability in Parks Fiberlink 210 firmware version V2.1.14_X000 was found via the /boaform/admin/formPing target_addr parameter.	7.2	More Details
CVE-2022-46738	The affected product exposes multiple sensitive data fields of the affected product. An attacker can use the SNMP command to get device mac address and login as admin.	7.2	More Details
CVE-2023-31742	There is a command injection vulnerability in the Linksys WRT54GL router with firmware version 4.30.18.006. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd s Start_EPI() function, thereby gaining shell privileges.	7.2	More Details
CVE-2023-31702	SQL injection in the View User Profile in MicroWorld eScan Management Console 14.0.1400.2281 allows remote attacker to dump entire database and gain windows XP command shell to perform code execution on database server via GetUserCurrentPwd? UsrId=1.	7.2	More Details
CVE-2023-31740	There is a command injection vulnerability in the Linksys E2000 router with firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post request parameters WL_atten_bb, WL_atten_radio, and WL_atten_ctl in the apply.cgi interface, thereby gaining shell privileges.	7.2	More Details
CVE-2023-31741	There is a command injection vulnerability in the Linksys E2000 router with firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ssid, wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd s Start_EPI() function, thereby gaining shell privileges.	7.2	More Details
CVE-2023-2756	SQL Injection in GitHub repository pimcore/customer-data-framework prior to 3.3.10.	7.2	More Details
CVE-2023-27512	Use of hard-coded credentials exists in SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10, and SV-CPT-MC310F versions prior to Ver.8.10, which may allow a remote authenticated attacker to login the affected product with an administrative privilege and perform an unintended operation.	7.2	More Details
CVE-2023-28392	Wi-Fi AP UNIT AC-PD-WAPU v1.05_B04 and earlier, AC-PD-WAPUM v1.05_B04 and earlier, AC-PD-WAPU-P v1.05_B04P and earlier, AC-PD-WAPUM-P v1.05_B04P and earlier, AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow an authenticated user with an administrative privilege to execute an arbitrary OS command.	7.2	More Details
CVE-2023-31245	Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device’s web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0864	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5.	7.1	More Details
CVE-2023-30487	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ThimPress LearnPress Export Import plugin <= 4.0.2 versions.	7.1	More Details
CVE-2023-30868	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Jon Christopher CMS Tree Page View plugin <= 1.6.7 versions.	7.1	More Details
CVE-2023-23890	Cross-Site Request Forgery (CSRF) vulnerability in LJ Apps WP Airbnb Review Slider plugin <= 3.2 versions.	7.1	More Details
CVE-2023-2509	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below.	7.1	More Details
CVE-2023-2597	In Eclipse Openj9 before version 0.38.0, in the implementation of the shared cache (which is enabled by default in OpenJ9 builds) the size of a string is not properly checked against the size of the buffer.	7.0	More Details
CVE-2023-25394	Videostream macOS app 0.5.0 and 0.4.3 has a Race Condition. The Updater privileged script attempts to update Videostream every 5 hours.	7.0	More Details
CVE-2023-28390	Privilege escalation vulnerability in SR-7100VN firmware Ver.1.38(N) and earlier and SR-7100VN #31 firmware Ver.1.21 and earlier allows a network-adjacent attacker with administrative privilege of the affected product to obtain an administrative privilege of the OS (Operating System). As a result, an arbitrary OS command may be executed.	6.8	More Details
CVE-2023-31756	A command injection vulnerability exists in the administrative web portal in TP-Link Archer VR1600V devices running firmware Versions <= 0.1.0. 0.9.1 v5006.0 Build 220518 Rel.32480n which allows remote attackers, authenticated to the administrative web portal as an administrator user to open an operating system level shell via the 'X_TP_IfName' parameter.	6.7	More Details
CVE-2020-36694	An issue was discovered in netfilter in the Linux kernel before 5.10. There can be a use-after-free in the packet processing context, because the per-CPU sequence count is mishandled during concurrent iptables rules replacement. This could be exploited with the CAP_NET_ADMIN capability in an unprivileged namespace. NOTE: cc00bca was reverted in 5.12.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30440	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175.	6.7	More Details
CVE-2023-23693	Dell VxRail, versions prior to 7.0.450, contains an OS command injection Vulnerability in DCManager command-line utility. A local high privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	6.7	More Details
CVE-2023-27066	Directory Traversal vulnerability in Site Core Experience Platform 10.2 and earlier allows authenticated remote attackers to download arbitrary files via Urlhandle.	6.5	More Details
CVE-2023-28623	Zulip is an open-source team collaboration tool with unique topic-based threading. In the event that 1: `ZulipLDAPAuthBackend` and an external authentication backend (any aside of `ZulipLDAPAuthBackend` and `EmailAuthBackend`) are the only ones enabled in `AUTHENTICATION_BACKENDS` in `/etc/zulip/settings.py` and 2: The organization permissions don't require invitations to join. An attacker can create a new account in the organization with an arbitrary email address in their control that's not in the organization's LDAP directory. The impact is limited to installations which have this specific combination of authentication backends as described above in addition to having `Invitations are required for joining this organization` organization permission disabled. This issue has been addressed in version 6.2. Users are advised to upgrade. Users unable to upgrade may enable the `Invitations are required for joining this organization` organization permission to prevent this issue.	6.5	More Details
CVE-2023-23667	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in BeRocket Brands for WooCommerce plugin <= 3.7.0.6 versions.	6.5	More Details
CVE-2023-20164	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2023-20163	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2023-31847	In davinci 0.3.0-rc after logging in, the user can connect to the mysql malicious server by controlling the data source to read arbitrary files on the client side.	6.5	More Details
CVE-2023-23999	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in MonsterInsights plugin <= 8.14.0 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33254	There is an LDAP bind credentials exposure on KACE Systems Deployment and Remote Site appliances 9.0.146. The captured credentials may provide a higher privilege level on the Active Directory domain. To exploit this, an authenticated attacker edits the user-authentication settings to specify an attacker-controlled LDAP server, clicks the Test Settings button, and captures the cleartext credentials.	6.5	More Details
CVE-2023-27921	JINS MEME CORE Firmware version 2.2.0 and earlier uses a hard-coded cryptographic key, which may lead to data acquired by a sensor of the affected product being decrypted by a network-adjacent attacker.	6.5	More Details
CVE-2023-33281	The remote keyfob system on Nissan Sylphy Classic 2021 sends the same RF signal for each door-open request, which allows for a replay attack. NOTE: the vendor's position is that this cannot be reproduced with genuine Nissan parts: for example, the combination of keyfob and door handle shown in the exploit demonstration does not match any technology that Nissan provides to customers.	6.5	More Details
CVE-2023-1764	Canon IJ Network Tool/Ver.4.7.5 and earlier (supported OS: OS X 10.9.5-macOS 13),IJ Network Tool/Ver.4.7.3 and earlier (supported OS: OS X 10.7.5-OS X 10.8) allows an attacker to acquire sensitive information on the Wi-Fi connection setup of the printer from the communication of the software.	6.5	More Details
CVE-2023-26595	Denial-of-service (DoS) vulnerability in Message of Cybozu Garoon 4.10.0 to 5.9.2 allows a remote authenticated attacker to cause a denial of service condition.	6.5	More Details
CVE-2023-1763	Canon IJ Network Tool/Ver.4.7.5 and earlier (supported OS: OS X 10.9.5-macOS 13),IJ Network Tool/Ver.4.7.3 and earlier (supported OS: OS X 10.7.5-OS X 10.8) allows an attacker to acquire sensitive information on the Wi-Fi connection setup of the printer from the software.	6.5	More Details
CVE-2023-30780	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TheGuideX User IP and Location plugin <= 2.2 versions.	6.5	More Details
CVE-2022-4945	The Dataprobe cloud usernames and passwords are stored in plain text in a specific file. Any user able to read this specific file from the device could compromise other devices connected to the user's cloud.	6.5	More Details
CVE-2023-31101	Insecure Default Initialization of Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.6.0. Users registered in InLong who joined later can see deleted users' data. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it.	6.5	More Details
CVE-2023-1972	A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20110	A vulnerability in the web-based management interface of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read sensitive data on the underlying database.	6.5	More Details
CVE-2022-46658	The affected product is vulnerable to a stack-based buffer overflow which could lead to a denial of service or remote code execution.	6.5	More Details
CVE-2023-31597	An issue in Zammad v5.4.0 allows attackers to bypass e-mail verification using an arbitrary address and manipulate the data of the generated user. Attackers are also able to gain unauthorized access to existing tickets.	6.5	More Details
CVE-2023-33203	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/emac/emac.c if a physically proximate attacker unplugs an emac based device.	6.4	More Details
CVE-2023-2799	A vulnerability, which was classified as problematic, has been found in cnoa OA up to 5.1.1.5. Affected by this issue is some unknown functionality of the file /index.php?app=main&func=passport&action=login. The manipulation leads to use of hard-coded password. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229376. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2769	A vulnerability classified as critical has been found in SourceCodester Service Provider Management System 1.0. This affects an unknown part of the file /classes/Master.php?f=delete_service. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229275.	6.3	More Details
CVE-2022-47609	Cross-Site Request Forgery (CSRF) vulnerability in Nicearma DNUI plugin <= 2.8.1 versions.	6.3	More Details
CVE-2023-2776	A vulnerability was found in code-projects Simple Photo Gallery 1.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-229282 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2775	A vulnerability was found in code-projects Bus Dispatch and Information System 1.0. It has been classified as critical. This affects an unknown part of the file adminHome.php. The manipulation of the argument reach_city 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-229281 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2773	A vulnerability has been found in code-projects Bus Dispatch and Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file view_admin.php. The manipulation of the argument adminid 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-229279.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2774	A vulnerability was found in code-projects Bus Dispatch and Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file view_branch.php. The manipulation of the argument branchid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229280.	6.3	More Details
CVE-2023-2823	A vulnerability was found in SourceCodester Class Scheduling System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_subject.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229597 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2771	A vulnerability, which was classified as critical, has been found in SourceCodester Online Exam System 1.0. This issue affects some unknown processing of the file /jurusanmatkul/data. The manipulation of the argument columns[1][data] 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-229277 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2772	A vulnerability, which was classified as critical, was found in SourceCodester Budget and Expense Tracker System 1.0. Affected is an unknown function of the file /admin/budget/manage_budget.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-229278 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2770	A vulnerability classified as critical was found in SourceCodester Online Exam System 1.0. This vulnerability affects unknown code of the file /kelasdosen/data. The manipulation of the argument columns[1][data] 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-229276.	6.3	More Details
CVE-2022-47984	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 243163.	6.3	More Details
CVE-2023-28045	Dell CloudIQ Collector version 1.10.2 contains a missing encryption of sensitive data vulnerability. An attacker with low privileges could potentially exploit this vulnerability, leading to gain access to unauthorized data.	6.3	More Details
CVE-2023-25707	Cross-Site Request Forgery (CSRF) vulnerability in E4J s.R.L. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.12 versions.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2815	A vulnerability classified as critical was found in SourceCodester Online Jewelry Store 1.0. Affected by this vulnerability is an unknown functionality of the file supplier.php of the component POST Parameter Handler. The manipulation of the argument suppid 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-229429 was assigned to this vulnerability.	6.3	More Details
CVE-2023-28514	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398.	6.2	More Details
CVE-2023-22878	IBM InfoSphere Information Server 11.7 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 244373.	6.2	More Details
CVE-2023-1996	A reflected Cross-site Scripting (XSS) vulnerability in Release 3DEXPERIENCE R2018x through Release 3DEXPERIENCE R2023x allows an attacker to execute arbitrary script code.	6.1	More Details
CVE-2023-25537	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	6.1	More Details
CVE-2023-31816	IT Sourcecode Content Management System Project In PHP and MySQL With Source Code 1.0.0 is vulnerable to Cross Site Scripting (XSS) via /ecodesource/search_list.php.	6.1	More Details
CVE-2022-45144	Algoo Tracim before 4.4.2 allows XSS via HTML file upload.	6.1	More Details
CVE-2023-27922	Cross-site scripting vulnerability in Newsletter versions prior to 7.6.9 allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2023-29837	Cross Site Scripting vulnerability found in Exelysis Unified Communication Solution (EUCS) v.1.0 allows a remote attacker to gain privileges via the URL path of the eucsAdmin login web page.	6.1	More Details
CVE-2023-31664	A reflected cross-site scripting (XSS) vulnerability in /authenticationendpoint/login.do of WSO2 API Manager before 4.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the tenantDomain parameter.	6.1	More Details
CVE-2023-33599	EasyImages2.0 ≤ 2.8.1 is vulnerable to Cross Site Scripting (XSS) via viewlog.php.	6.1	More Details
CVE-2023-28467	In MyBB before 1.8.34, there is XSS in the User CP module via the user email field.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31584	GitHub repository cu/silicon commit a9ef36 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the User Input field.	6.1	More Details
CVE-2023-29720	SofaWiki <=3.8.9 is vulnerable to Cross Site Scripting (XSS) via index.php.	6.1	More Details
CVE-2023-20167	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.0	More Details
CVE-2023-20166	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.0	More Details
CVE-2023-32515	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Matt Gibbs Custom Field Suite plugin <= 2.6.2.1 versions.	5.9	More Details
CVE-2023-31233	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Haoqisir Baidu Tongji generator plugin <= 1.0.2 versions.	5.9	More Details
CVE-2022-47157	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Don Benjamin WP Custom Fields Search plugin <= 1.2.34 versions.	5.9	More Details
CVE-2022-36328	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could allow an attacker to create arbitrary shares on arbitrary directories and exfiltrate sensitive files, passwords, users and device configurations was discovered in Western Digital My Cloud Home, My Cloud Home Duo, SanDisk ibi and Western Digital My Cloud OS 5 devices. This can only be exploited once an attacker gains root privileges on the devices using an authentication bypass issue or another vulnerability.This issue affects My Cloud Home and My Cloud Home Duo: before 9.4.0-191; ibi: before 9.4.0-191; My Cloud OS 5: before 5.26.202.	5.8	More Details
CVE-2022-36327	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could allow an attacker to write files to locations with certain critical filesystem types leading to remote code execution was discovered in Western Digital My Cloud Home, My Cloud Home Duo, SanDisk ibi and Western Digital My Cloud OS 5 devices. This issue requires an authentication bypass issue to be triggered before this can be exploited. This issue affects My Cloud Home and My Cloud Home Duo: before 9.4.0-191; ibi: before 9.4.0-191; My Cloud OS 5: before 5.26.202.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32680	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but affected versions of Metabase didn't enforce that requirement. This lack of enforcement meant that: Anyone–including people in sandboxed groups–could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the snippet contained logic that restricted which data that person could see, they could potentially edit that snippet and change their level of data access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that SQL queries used to create sandboxes exclude SQL snippets.	5.8	More Details
CVE-2023-32348	Teltonika's Remote Management System versions prior to 4.10.0 contain a virtual private network (VPN) hub feature for cross-device communication that uses OpenVPN. It connects new devices in a manner that allows the new device to communicate with all Teltonika devices connected to the VPN. The OpenVPN server also allows users to route through it. An attacker could route a connection to a remote server through the OpenVPN server, enabling them to scan and access data from other Teltonika devices connected to the VPN.	5.8	More Details
CVE-2023-2782	Sensitive information disclosure due to improper authorization. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.3.1-38.	5.5	More Details
CVE-2023-30775	A vulnerability was found in the libtiff library. This security flaw causes a heap buffer overflow in extractContigSamples32bits, tiffcrop.c.	5.5	More Details
CVE-2023-31518	A heap use-after-free in the component CDataFileReader::GetItem of teeworlds v0.7.5 allows attackers to cause a Denial of Service (DoS) via a crafted map file.	5.5	More Details
CVE-2023-30774	A vulnerability was found in the libtiff library. This flaw causes a heap buffer overflow issue via the TIFFTAG_INKNAMES and TIFFTAG_NUMBEROFINKS values.	5.5	More Details
CVE-2023-26818	Telegram 9.3.1 and 9.4.0 allows attackers to access restricted files, microphone ,or video recording via the DYLD_INSERT_LIBRARIES flag.	5.5	More Details
CVE-2023-2731	A NULL pointer dereference flaw was found in Libtiff's LZWDecode() function in the libtiff/tif_lzw.c file. This flaw allows a local attacker to craft specific input data that can cause the program to dereference a NULL pointer when decompressing a TIFF format file, resulting in a program crash or denial of service.	5.5	More Details
CVE-2023-2837	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.2.2.	5.5	More Details
CVE-2023-1195	A use-after-free flaw was found in reconn_set_ipaddr_from_hostname in fs/cifs/connect.c in the Linux kernel. The issue occurs when it forgets to set the free pointer server->hostname to NULL, leading to an invalid pointer request.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31725	yasm 1.3.0.55.g101bc was discovered to contain a heap-use-after-free via the function expand_mmac_params at yasm/modules/preprocs/nasm/nasm-pp.c.	5.5	More Details
CVE-2023-2806	A vulnerability classified as problematic was found in Weaver e-cology up to 9.0. Affected by this vulnerability is the function RequestInfoByXml of the component API. The manipulation leads to xml external entity reference. The associated identifier of this vulnerability is VDB-229411. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-28529	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 251213.	5.5	More Details
CVE-2023-31669	WebAssembly wat2wasm v1.0.32 allows attackers to cause a libc++abi.dylib crash by putting '@' before a quote (").	5.5	More Details
CVE-2023-31723	yasm 1.3.0.55.g101bc was discovered to contain a segmentation violation via the function expand_mmac_params at /nasm/nasm-pp.c.	5.5	More Details
CVE-2023-20182	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2023-25440	Stored Cross Site Scripting (XSS) vulnerability in the add contact function CiviCRM 5.59.alpha1, allows attackers to execute arbitrary code in first/second name field.	5.4	More Details
CVE-2023-20183	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2023-31779	Wekan v6.84 and earlier is vulnerable to Cross Site Scripting (XSS). An attacker with user privilege on kanban board can insert JavaScript code in in "Reaction to comment" feature.	5.4	More Details
CVE-2023-30124	LavaLite v9.0.0 is vulnerable to Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-30452	The MoroSystems EasyMind - Mind Maps plugin before 2.15.0 for Confluence allows persistent XSS when saving a Mind Map with the hyperlink parameter.	5.4	More Details
CVE-2023-25448	Cross-Site Request Forgery (CSRF) vulnerability in Eric Teubert Archivist – Custom Archive Templates plugin <= 1.7.4 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20184	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2022-47183	Cross-Site Request Forgery (CSRF) vulnerability in StylistWP Extra Block Design, Style, CSS for ANY Gutenberg Blocks plugin <= 0.2.6 versions.	5.4	More Details
CVE-2023-31860	Wuzhi CMS v3.1.2 has a storage type XSS vulnerability in the backend of the Five Finger CMS b2b system.	5.4	More Details
CVE-2023-25481	Cross-Site Request Forgery (CSRF) vulnerability in Podlove Podlove Subscribe button plugin <= 1.3.7 versions.	5.4	More Details
CVE-2023-23712	Cross-Site Request Forgery (CSRF) vulnerability in User Meta Manager plugin <= 3.4.9 versions.	5.4	More Details
CVE-2022-47167	Cross-Site Request Forgery (CSRF) vulnerability in Aram Kocharyan Crayon Syntax Highlighter plugin <= 2.8.4 versions.	5.4	More Details
CVE-2023-2752	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta.	5.4	More Details
CVE-2023-2716	The Groundhogg plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the 'ajax_upload_file' function in versions up to, and including, 2.7.9.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload a file to the contact, and then lists all the other uploaded files related to the contact.	5.4	More Details
CVE-2023-2717	The Groundhogg plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.7.9.8. This is due to missing nonce validation on the 'enable_safe_mode' function. This makes it possible for unauthenticated attackers to enable safe mode, which disables all other plugins, via a forged request if they can successfully trick an administrator into performing an action such as clicking on a link. A warning message about safe mode is displayed to the admin, which can be easily disabled.	5.4	More Details
CVE-2023-2528	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-20172	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20171	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2023-22689	Cross-Site Request Forgery (CSRF) vulnerability in Lucian Apostol Auto Affiliate Links plugin <= 6.3 versions.	5.4	More Details
CVE-2023-28367	Cross-site scripting vulnerability in CTA post function of VK All in One Expansion Unit 9.88.1.0 and earlier allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-27926	Cross-site scripting vulnerability in Profile setting function of VK All in One Expansion Unit 9.88.1.0 and earlier allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-27925	Cross-site scripting vulnerability in Post function of VK Blocks 1.53.0.1 and earlier and VK Blocks Pro 1.53.0.1 and earlier allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2021-46888	An issue was discovered in hledger before 1.23. A Stored Cross-Site Scripting (XSS) vulnerability exists in toBloodhoundJson that allows an attacker to execute JavaScript by encoding user-controlled values in a payload with base64 and parsing them with the atob function.	5.4	More Details
CVE-2023-27923	Cross-site scripting vulnerability in Tag edit function of VK Blocks 1.53.0.1 and earlier and VK Blocks Pro 1.53.0.1 and earlier allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2023-20106	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2023-27430	Cross-Site Request Forgery (CSRF) vulnerability in Ramon Fincken Mass Delete Unused Tags plugin <= 2.0.0 versions.	5.4	More Details
CVE-2023-23797	Cross-Site Request Forgery (CSRF) vulnerability in SecondLineThemes Auto YouTube Importer plugin <= 1.0.3 versions.	5.4	More Details
CVE-2023-2753	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta.	5.4	More Details
CVE-2023-23680	Cross-Site Request Forgery (CSRF) vulnerability in Bob Goetz WP-TopBar plugin <= 5.36 versions.	5.4	More Details
CVE-2023-25698	Cross-Site Request Forgery (CSRF) vulnerability in Studio Wombat Shoppable Images plugin <= 1.2.3 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27423	Cross-Site Request Forgery (CSRF) vulnerability in Ramon Fincken Auto Prune Posts plugin <= 1.8.0 versions.	5.4	More Details
CVE-2023-31757	DedeCMS up to v5.7.108 is vulnerable to XSS in sys_info.php via parameters 'edit___cfg_powerby' and 'edit___cfg_beian'	5.4	More Details
CVE-2023-31862	jizhicms v2.4.6 is vulnerable to Cross Site Scripting (XSS). The content of the article published in the front end is only filtered in the front end, without being filtered in the background, which allows attackers to publish an article containing malicious JavaScript scripts by modifying the request package.	5.4	More Details
CVE-2022-41608	Cross-Site Request Forgery (CSRF) vulnerability in Thomas Belser Asgaros Forum plugin <= 2.2.0 versions.	5.4	More Details
CVE-2023-22654	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	5.4	More Details
CVE-2023-2745	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the ‘wp_lang’ parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.	5.4	More Details
CVE-2023-31698	Bludit v3.14.1 is vulnerable to Stored Cross Site Scripting (XSS) via SVG file on site logo. NOTE: the product's security model is that users are trusted by the administrator to insert arbitrary content (users cannot create their own accounts through self-registration).	5.4	More Details
CVE-2023-23813	Cross-Site Request Forgery (CSRF) vulnerability in Joseph C Dolson My Calendar plugin <= 3.4.3 versions.	5.4	More Details
CVE-2023-31995	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-31994	Certain Hanwha products are vulnerable to Denial of Service (DoS). ck vector is: When an empty UDP packet is sent to the listening service, the service thread results in a non-functional service (DoS) via WS Discovery and Hanwha proprietary discovery services. This affects IP Camera ANE-L7012R 1.41.01 and IP Camera XNV-9082R 2.10.02.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26044	react/http is an event-driven, streaming HTTP client and server implementation for ReactPHP. Previous versions of ReactPHP's HTTP server component contain a potential DoS vulnerability that can cause high CPU load when processing large HTTP request bodies. This vulnerability has little to no impact on the default configuration, but can be exploited when explicitly using the RequestBodyBufferMiddleware with very large settings. This might lead to consuming large amounts of CPU time for processing requests and significantly delay or slow down the processing of legitimate user requests. This issue has been addressed in release 1.9.0. Users are advised to upgrade. Users unable to upgrade may keep the request body limited using RequestBodyBufferMiddleware with a sensible value which should mitigate the issue. An infrastructure or DevOps workaround could be to place a reverse proxy in front of the ReactPHP HTTP server to filter out any excessive HTTP request bodies.	5.3	More Details
CVE-2023-28015	The HCL Domino AppDev Pack IAM service is susceptible to a User Account Enumeration vulnerability. During a failed login attempt a difference in messages could allow an attacker to determine if the user is valid or not. The attacker could use this information to focus a brute force attack on valid users.	5.3	More Details
CVE-2023-23545	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	5.3	More Details
CVE-2023-28412	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	5.3	More Details
CVE-2023-2766	A vulnerability was found in Weaver OA 9.5 and classified as problematic. This issue affects some unknown processing of the file /building/backmgr/urlpage/mobileurl/configfile/jx2_config.ini. The manipulation leads to files or directories accessible. 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-229271. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-32098	Compiler removal of buffer clearing in sli_se_sign_message in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	5.3	More Details
CVE-2023-32346	Teltonika’s Remote Management System versions prior to 4.10.0 contain a function that allows users to claim their devices. This function returns information based on whether the serial number of a device has already been claimed, the MAC address of a device has already been claimed, or whether the attempt to claim a device was successful. An attacker could exploit this to create a list of the serial numbers and MAC addresses of all devices cloud-connected to the Remote Management System.	5.3	More Details
CVE-2022-4870	In affected versions of Octopus Deploy it is possible to discover network details via error message	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1132	Compiler removal of buffer clearing in sli_se_driver_key_agreement in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	5.3	More Details
CVE-2023-33285	An issue was discovered in Qt 5.x before 5.15.14, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. QDnsLookup has a buffer over-read via a crafted reply from a DNS server.	5.3	More Details
CVE-2023-2481	Compiler removal of buffer clearing in sli_se_opaque_import_key in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	5.3	More Details
CVE-2023-29857	An issue in Teslamate v1.27.1 allows attackers to obtain sensitive information via directly accessing the teslamate link.	5.3	More Details
CVE-2022-44739	Cross-Site Request Forgery (CSRF) vulnerability in ThingsForRestaurants Quick Restaurant Reservations plugin <= 1.5.4 versions.	5.3	More Details
CVE-2023-32100	Compiler removal of buffer clearing in sli_se_driver_mac_compute in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	5.3	More Details
CVE-2023-32099	Compiler removal of buffer clearing in sli_se_sign_hash in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	5.3	More Details
CVE-2023-33293	An issue was discovered in KaiOS 3.0 and 3.1. The binary /system/kaios/api-daemon exposes a local web server on *.localhost with subdomains for each installed applications, e.g., myapp.localhost. An attacker can make fetch requests to api-deamon to determine if a given app is installed and read the manifest.webmanifest contents, including the app version.	5.3	More Details
CVE-2023-28950	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358.	5.1	More Details
CVE-2023-2025	OpenBlue Enterprise Manager Data Collector versions prior to 3.2.5.75 may expose sensitive information to an unauthorized user under certain circumstances.	5.0	More Details
CVE-2023-2735	The Groundhogg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gh_form' shortcode in versions up to, and including, 2.7.9.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Please note this only works with legacy contact forms.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32322	Ombi is an open source application which allows users to request specific media from popular self-hosted streaming servers. Versions prior to 4.38.2 contain an arbitrary file read vulnerability where an Ombi administrative user may access files available to the Ombi server process on the host operating system. Ombi administrators may not always be local system administrators and so this may violate the security expectations of the system. The arbitrary file read vulnerability was present in `ReadLogFile` and `Download` endpoints in `SystemControllers.cs` as the parameter `logFileName` is not sanitized before being combined with the `Logs` directory. When using `Path.Combine(arg1, arg2, arg3)`, an attacker may be able to escape to folders/files outside of `Path.Combine(arg1, arg2)` by using ".." in `arg3`. In addition, by specifying an absolute path for `arg3`, `Path.Combine` will completely ignore the first two arguments and just return just `arg3`. This vulnerability can lead to information disclosure. The Ombi `documentation` suggests running Ombi as a Service with Administrator privileges. An attacker targeting such an application may be able to read the files of any Windows user on the host machine and certain system files. This issue has been addressed in commit `b8a8f029` and in release version 4.38.2. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GHSL-2023-088.	4.9	More Details
CVE-2023-2844	Authorization Bypass Through User-Controlled Key in GitHub repository cloudexplorer-dev/cloudexplorer-lite prior to v1.1.0.	4.9	More Details
CVE-2023-20077	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device.	4.9	More Details
CVE-2023-20174	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	4.9	More Details
CVE-2023-20087	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device.	4.9	More Details
CVE-2023-20173	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31699	ChurchCRM v4.5.4 is vulnerable to Reflected Cross-Site Scripting (XSS) via image file.	4.8	More Details
CVE-2023-1859	A use-after-free flaw was found in xen_9pfs_front_removet in net/9p/trans_xen.c in Xen transport for 9pfs in the Linux Kernel. This flaw could allow a local attacker to crash the system due to a race problem, possibly leading to a kernel information leak.	4.7	More Details
CVE-2023-23694	Dell VxRail versions earlier than 7.0.450, contain(s) an OS command injection vulnerability in VxRail Manager. A local authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	4.7	More Details
CVE-2023-20003	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication.	4.7	More Details
CVE-2023-33251	When Akka HTTP before 10.5.2 accepts file uploads via the FileUploadDirectives.fileUploadAll directive, the temporary file it creates has too weak permissions: it is readable by other users on Linux or UNIX, a similar issue to CVE-2022-41946.	4.7	More Details
CVE-2023-33288	An issue was discovered in the Linux kernel before 6.2.9. A use-after-free was found in bq24190_remove in drivers/power/supply/bq24190_charger.c. It could allow a local attacker to crash the system due to a race condition.	4.7	More Details
CVE-2023-2800	Insecure Temporary File in GitHub repository huggingface/transformers prior to 4.30.0.	4.7	More Details
CVE-2023-33250	The Linux kernel 6.3 has a use-after-free in iopt_unmap_iova_range in drivers/iommu/iommufd/io_pagetable.c.	4.4	More Details
CVE-2022-36326	An uncontrolled resource consumption vulnerability issue that could arise by sending crafted requests to a service to consume a large amount of memory, eventually resulting in the service being stopped and restarted was discovered in Western Digital My Cloud Home, My Cloud Home Duo, SanDisk ibi and Western Digital My Cloud OS 5 devices. This issue requires the attacker to already have root privileges in order to exploit this vulnerability.This issue affects My Cloud Home and My Cloud Home Duo: before 9.4.0-191; ibi: before 9.4.0-191; My Cloud OS 5: before 5.26.202.	4.4	More Details
CVE-2023-23706	Cross-Site Request Forgery (CSRF) vulnerability in miniOrange WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin <= 7.5.14 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2715	The Groundhogg plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'submit_ticket' function in versions up to, and including, 2.7.9.8. This makes it possible for authenticated attackers to create a support ticket that sends the website's data to the plugin developer, and it is also possible to create an admin access with an auto login link that is also sent to the plugin developer with the ticket. It only works if the plugin is activated with a valid license.	4.3	More Details
CVE-2023-23724	Cross-Site Request Forgery (CSRF) vulnerability in Winwar Media WP Email Capture plugin <= 3.9.3 versions.	4.3	More Details
CVE-2023-23705	Cross-Site Request Forgery (CSRF) vulnerability in HM Plugin WordPress Books Gallery plugin <= 4.4.8 versions.	4.3	More Details
CVE-2023-25472	Cross-Site Request Forgery (CSRF) vulnerability in Podlove Podlove Podcast Publisher plugin <= 3.8.3 versions.	4.3	More Details
CVE-2023-2714	The Groundhogg plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'check_license' functions in versions up to, and including, 2.7.9.8. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to change the license key and support license key, but it can only be changed to a valid license key.	4.3	More Details
CVE-2022-46851	Cross-Site Request Forgery (CSRF) vulnerability in Brainstorm Force Starter Templates plugin <= 3.1.20 versions.	4.3	More Details
CVE-2022-46853	Cross-Site Request Forgery (CSRF) vulnerability in RadiusTheme The Post Grid plugin <= 5.0.4 versions.	4.3	More Details
CVE-2023-23713	Cross-Site Request Forgery (CSRF) vulnerability in Manoj Thulasidas Theme Tweaker plugin <= 5.20 versions.	4.3	More Details
CVE-2023-25056	Cross-Site Request Forgery (CSRF) vulnerability in SlickRemix Feed Them Social plugin <= 3.0.2 versions.	4.3	More Details
CVE-2023-33359	Piwigo 13.6.0 is vulnerable to Cross Site Request Forgery (CSRF) in the "add tags" function.	4.3	More Details
CVE-2022-46813	Cross-Site Request Forgery (CSRF) vulnerability in Younes JFR. Advanced Database Cleaner plugin <= 3.1.1 versions.	4.3	More Details
CVE-2023-26011	Cross-Site Request Forgery (CSRF) vulnerability in Tim Eckel Read More Excerpt Link plugin <= 1.6 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26014	Cross-Site Request Forgery (CSRF) vulnerability in Tim Eckel Minify HTML plugin <= 2.1.7 vulnerability.	4.3	More Details
CVE-2023-25474	Cross-Site Request Forgery (CSRF) vulnerability in Csaba Kissi About Me 3000 widget plugin <= 2.2.6 versions.	4.3	More Details
CVE-2023-1209	Cross-Site Scripting (XSS) vulnerabilities exist in ServiceNow records allowing an authenticated attacker to inject arbitrary scripts.	4.3	More Details
CVE-2023-2822	A vulnerability was found in Ellucian Ethos Identity up to 5.10.5. It has been classified as problematic. Affected is an unknown function of the file /cas/logout. The manipulation of the argument url leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 5.10.6 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-229596.	4.3	More Details
CVE-2023-24414	Cross-Site Request Forgery (CSRF) vulnerability in RoboSoft Photo Gallery, Images, Slider in Rbs Image Gallery plugin <= 3.2.11 versions.	4.3	More Details
CVE-2022-45079	Cross-Site Request Forgery (CSRF) vulnerability in Softaculous Loginizer plugin <= 1.7.5 versions.	4.3	More Details
CVE-2022-47611	Cross-Site Request Forgery (CSRF) vulnerability in Julian Weinert // cs&m Hover Image plugin <= 1.4.1 versions.	4.3	More Details
CVE-2022-45376	Cross-Site Request Forgery (CSRF) vulnerability in XootiX Side Cart Woocommerce (Ajax) < 2.1 versions.	4.3	More Details
CVE-2023-31708	A Cross-Site Request Forgery (CSRF) in EyouCMS v1.6.2 allows attackers to execute arbitrary commands via a supplying a crafted HTML file to the Upload software format function.	4.3	More Details
CVE-2022-45076	Cross-Site Request Forgery (CSRF) vulnerability in WebMat Flexible Elementor Panel plugin <= 2.3.8 versions.	4.3	More Details
CVE-2023-22714	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Coming Soon by Supsystic plugin <= 1.7.10 versions.	4.3	More Details
CVE-2023-22709	Cross-Site Request Forgery (CSRF) vulnerability in Atif N SRS Simple Hits Counter plugin <= 1.1.0 versions.	4.3	More Details
CVE-2023-22692	Cross-Site Request Forgery (CSRF) vulnerability in Jeroen Peters Name Directory plugin <= 1.27.1 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22688	Cross-Site Request Forgery (CSRF) vulnerability in Abdul Ibad WP Tabs Slides plugin <= 2.0.3 versions.	4.3	More Details
CVE-2022-47142	Cross-Site Request Forgery (CSRF) vulnerability in Plugincraft Mediamatic – Media Library Folders plugin <= 2.8.1 versions.	4.3	More Details
CVE-2023-22348	Improper Authorization in RestAPI in Checkmk GmbH's Checkmk versions <2.1.0p28 and <2.2.0b8 allows remote authenticated users to read arbitrary host_configs.	4.3	More Details
CVE-2023-25447	Cross-Site Request Forgery (CSRF) vulnerability in Inkthemescom ColorWay theme <= 4.2.3 versions.	4.3	More Details
CVE-2023-27304	Operation restriction bypass vulnerability in Message and Bulletin of Cybozu Garoon 4.6.0 to 5.9.2 allows a remote authenticated attacker to alter the data of Message and/or Bulletin.	4.3	More Details
CVE-2023-27384	Operation restriction bypass vulnerability in MultiReport of Cybozu Garoon 5.15.0 allows a remote authenticated attacker to alter the data of MultiReport.	4.3	More Details
CVE-2023-2765	A vulnerability has been found in Weaver OA up to 9.5 and classified as problematic. This vulnerability affects unknown code of the file /E-mobile/App/System/File/downfile.php. The manipulation of the argument url leads to absolute path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-229270 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-27920	Improper access control vulnerability in the system date/time setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to alter system date/time of the affected product.	4.3	More Details
CVE-2023-33264	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, configuration routines don't mask passwords in the member configuration properly. This allows Hazelcast Management Center users to view some of the secrets.	4.3	More Details
CVE-2023-32589	Cross-Site Request Forgery (CSRF) vulnerability in PingOnline Dyslexiefont Free plugin <= 1.0.0 versions.	4.3	More Details
CVE-2022-47134	Cross-Site Request Forgery (CSRF) vulnerability in Bill Erickson Gallery Metabox plugin <= 1.5 versions.	4.3	More Details
CVE-2023-2679	Data leakage in Adobe connector in Snow Software SPE 9.27.0 on Windows allows privileged user to observe other users data.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32675	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. In contracts with more than one regular nonpayable function, it is possible to send funds to the default function, even if the default function is marked `nonpayable`. This applies to contracts compiled with vyper versions prior to 0.3.8. This issue was fixed by the removal of the global `calldatasize` check in commit `02339dfda`. Users are advised to upgrade to version 0.3.8. Users unable to upgrade should avoid use of nonpayable default functions.	3.7	More Details
CVE-2023-2768	A vulnerability was found in Sucms 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin_ads.php?action=add. The manipulation of the argument intro leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-229274 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-2789	A vulnerability was found in GNU cflow 1.7. It has been rated as problematic. This issue affects the function func_body/parse_variable_declaration of the file parser.c. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. The identifier VDB-229373 was 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-2023-2824	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/service.php of the component POST Parameter Handler. The manipulation of the argument service leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-229598 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-2814	A vulnerability classified as problematic has been found in SourceCodester Class Scheduling System 1.0. Affected is an unknown function of the file /admin/save_teacher.php of the component POST Parameter Handler. The manipulation of the argument Academic_Rank leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229428.	3.5	More Details
CVE-2023-2826	A vulnerability has been found in SourceCodester Class Scheduling System 1.0 and classified as problematic. This vulnerability affects unknown code of the file search_teacher_result.php of the component POST Parameter Handler. The manipulation of the argument teacher leads to cross site scripting. 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-229612.	3.5	More Details
CVE-2022-35798	Azure Arc Jumpstart Information Disclosure Vulnerability	3.3	More Details
CVE-2023-28369	Brother iPrint&Scan V6.11.2 and earlier contains an improper access control vulnerability. This vulnerability may be exploited by the other app installed on the victim user's Android device, which may lead to displaying the settings and/or log information of the affected app as a print preview.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42336	Mishandling of guest SSBD selection on AMD hardware The current logic to set SSBD on AMD Family 17h and Hygon Family 18h processors requires that the setting of SSBD is coordinated at a core level, as the setting is shared between threads. Logic was introduced to keep track of how many threads require SSBD active in order to coordinate it, such logic relies on using a per-core counter of threads that have SSBD active. When running on the mentioned hardware, it's possible for a guest to under or overflow the thread counter, because each write to VIRT_SPEC_CTRL.SSBD by the guest gets propagated to the helper that does the per-core active accounting. Underflowing the counter causes the value to get saturated, and thus attempts for guests running on the same core to set SSBD won't have effect because the hypervisor assumes it's already active.	3.3	More Details
CVE-2023-31135	Dgraph is an open source distributed GraphQL database. Existing Dgraph audit logs are vulnerable to brute force attacks due to nonce collisions. The first 12 bytes come from a baseIv which is initialized when an audit log is created. The last 4 bytes come from the length of the log line being encrypted. This is problematic because two log lines will often have the same length, so due to these collisions we are reusing the same nonce many times. All audit logs generated by versions of Dgraph <v23.0.0 are affected. Attackers must have access to the system the logs are stored on. Dgraph users should upgrade to v23.0.0. Users unable to upgrade should store existing audit logs in a secure location and for extra security, encrypt using an external tool like `gpg`.	3.3	More Details
CVE-2023-2608	The Multiple Page Generator Plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 3.3.17 due to missing nonce verification on the projects_list function and insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries leading to resource exhaustion via a forged request granted they can trick an administrator into performing an action such as clicking on a link. Version 3.3.18 addresses the SQL Injection, which drastically reduced the severity.	3.1	More Details
CVE-2023-32677	Zulip is an open-source team collaboration tool with unique topic-based threading. Zulip administrators can configure Zulip to limit who can add users to streams, and separately to limit who can invite users to the organization. In Zulip Server 6.1 and below, the UI which allows a user to invite a new user also allows them to set the streams that the new user is invited to -- even if the inviting user would not have permissions to add an existing user to streams. While such a configuration is likely rare in practice, the behavior does violate security-related controls. This does not let a user invite new users to streams they cannot see, or would not be able to add users to if they had that general permission. This issue has been addressed in version 6.2. Users are advised to upgrade. Users unable to upgrade may limit sending of invitations down to users who also have the permission to add users to streams.	3.1	More Details
CVE-2023-32096	Compiler removal of buffer clearing in sli_crypto_transparent_aead_encrypt_tag in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	3.1	More Details
CVE-2023-32097	Compiler removal of buffer clearing in sli_crypto_transparent_aead_decrypt_tag in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0965	Compiler removal of buffer clearing in sli_cryptoacc_transparent_key_agreement in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	3.1	More Details
CVE-2023-2790	A vulnerability classified as problematic has been found in TOTOLINK N200RE 9.3.5u.6255_B20211224. Affected is an unknown function of the file /squashfs-root/etc_ro/custom.conf of the component Telnet Service. The manipulation leads to password in configuration file. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-229374 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.3	More Details
CVE-2023-2469	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-2483	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-33203. Reason: This candidate is a reservation duplicate of CVE-2023-33203. Notes: All CVE users should reference CVE-2023-33203 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details