SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 February 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-23603	iTunesRPC-Remastered is a discord rich presence application for use with iTunes & Apple Music. In code before commit 24f43aa user input is not properly sanitized and code injection is possible. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue.	9.9	More Details
CVE-2021-23484	The package zip-local before 0.3.5 are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) which can lead to an extraction of a crafted file outside the intended extraction directory.	9.8	More Details
CVE-2021-46444	H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/admin.php?module=admin_group_edit&agID.	9.8	More Details
CVE-2021-46445	H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/categories.php?box_group_id.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46446	H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/admin.php?module=admin_access_group_edit&aagID.	9.8	More Details
CVE-2021-46448	H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/customers.php?page=1&cID.	9.8	More Details
CVE-2021-46660	Signiant Manager+Agents before 15.1 allows XML External Entity (XXE) attacks.	9.8	More Details
CVE-2022-0339	Server-Side Request Forgery (SSRF) in Pypi calibreweb prior to 0.6.16.	9.8	More Details
CVE-2020-36064	Online Course Registration v1.0 was discovered to contain hardcoded credentials in the source code which allows attackers access to the control panel if compromised.	9.8	More Details
CVE-2021-31617	In ASQ in Stormshield Network Security (SNS) 1.0.0 through 2.7.8, 2.8.0 through 2.16.0, 3.0.0 through 3.7.20, 3.8.0 through 3.11.8, and 4.0.1 through 4.2.2, mishandling of memory management can lead to remote code execution.	9.8	More Details
CVE-2022-24263	Hospital Management System v4.0 was discovered to contain a SQL injection vulnerability in /Hospital-Management-System-master/func.php via the email parameter.	9.8	More Details
CVE-2021-24762	The Perfect Survey WordPress plugin before 1.5.2 does not validate and escape the question_id GET parameter before using it in a SQL statement in the get_question AJAX action, allowing unauthenticated users to perform SQL injection.	9.8	More Details
CVE-2022-21217	An out-of-bounds write vulnerability exists in the device TestEmail functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted network request can lead to an out-of-bounds write. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2022-0320	The Essential Addons for Elementor WordPress plugin before 5.0.5 does not validate and sanitise some template data before it them in include statements, which could allow unauthenticated attackers to perform Local File Inclusion attack and read arbitrary files on the server, this could also lead to RCE via user uploaded files or other LFI to RCE techniques.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0401	Path Traversal in NPM w-zip prior to 1.0.12.	9.8	More Details
CVE-2021-43509	SQL Injection vulnerability exists in Sourcecodester Simple Client Management System 1.0 via the id parameter in view-service.php.	9.8	More Details
CVE-2021-43510	SQL Injection vulnerability exists in Sourcecodester Simple Client Management System 1.0 via the username field in login.php.	9.8	More Details
CVE-2021-46093	eliteCMS v1.0 is vulnerable to Insecure Permissions via manage_uploads.php.	9.8	More Details
CVE-2022-24219	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_page.php.	9.8	More Details
CVE-2022-24220	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_post.php.	9.8	More Details
CVE-2022-24221	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/functions/functions.php.	9.8	More Details
CVE-2022-24222	eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_user.php.	9.8	More Details
CVE-2021-46560	The firmware on Moxa TN-5900 devices through 3.1 allows command injection that could lead to device damage.	9.8	More Details
CVE-2022-24223	AtomCMS v2.0 was discovered to contain a SQL injection vulnerability via /admin/login.php.	9.8	More Details
CVE-2021-40409	An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->password variable, that has the value of the password parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45898	SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows local file inclusion.	9.8	More Details
CVE-2022-0362	SQL Injection in Packagist showdoc/showdoc prior to 2.10.3.	9.8	More Details
CVE-2021-46386	File upload vulnerability in mingSoft MCMS through 5.2.5, allows remote attackers to execute arbitrary code via a crafted jspx webshell to net.mingsoft.basic.action.web.FileAction#upload.	9.8	More Details
CVE-2021-46377	There is a front-end sql injection vulnerability in cszcms 1.2.9 via cszcms/controllers/Member.php#viewUser	9.8	More Details
CVE-2021-46427	An SQL Injection vulnerability exists in Sourcecodester Simple Chatbot Application 1.0 via the message parameter in Master.php.	9.8	More Details
CVE-2021-46428	A Remote Code Execution (RCE) vulnerability exists in Sourcecodester Simple Chatbot Application 1.0 (and previous versions via the bot_avatar parameter in SystemSettings.php.	9.8	More Details
CVE-2021-44249	Online Motorcycle (Bike) Rental System 1.0 is vulnerable to a Blind Time-Based SQL Injection attack within the login portal. This can lead attackers to remotely dump MySQL database credentials.	9.8	More Details
CVE-2021-45435	An SQL Injection vulnerability exists in Sourcecodester Simple Cold Storage Management System using PHP/OOP 1.0 via the username field in login.php.	9.8	More Details
CVE-2021-40408	An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->username variable, that has the value of the userName parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection.	9.8	More Details
CVE-2020-25905	An SQL Injection vulnerabilty exists in Sourcecodester Mobile Shop System in PHP MySQL 1.0 via the email parameter in (1) login.php or (2) LoginAsAdmin.php.	9.8	More Details
CVE-2021-45899	SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows PHAR deserialization that can lead to remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22294	A SQL injection vulnerability exists in ZFAKA<=1.43 which an attacker can use to complete SQL injection in the foreground and add a background administrator account.	9.8	More Details
CVE-2021-41609	SQL injection in the ID parameter of the UploadedImageDisplay.aspx endpoint of SelectSurvey.NET before 5.052.000 allows a remote, unauthenticated attacker to retrieve data from the application's backend database via boolean-based blind and UNION injection.	9.8	More Details
CVE-2021-44971	Multiple Tenda devices are affected by authentication bypass, such as AC15V1.0 Firmware V15.03.05.20_multi?AC5V1.0 Firmware V15.03.06.48_multi and so on. an attacker can obtain sensitive information, and even combine it with authenticated command injection to implement RCE.	9.8	More Details
CVE-2021-22820	A CWE-614 Insufficient Session Expiration vulnerability exists that could allow an attacker to maintain an unauthorized access over a hijacked session to the charger station web server even after the legitimate user account holder has changed his password. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	9.8	More Details
CVE-2021-40407	An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->domain variable, that has the value of the domain parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-24814	The check_privacy_settings AJAX action of the WordPress GDPR WordPress plugin before 1.9.26, available to both unauthenticated and authenticated users, responds with JSON data without an "application/json" content-type. Since an HTML payload isn't properly escaped, it may be interpreted by a web browser led to this endpoint. Javascript code may be executed on a victim's browser. If the victim is an administrator with a valid session cookie, full control of the WordPress instance may be taken (AJAX calls and iframe manipulation are possible because the vulnerable endpoint is on the same domain as the admin panel - there is no same-origin restriction).	9.6	More Details
CVE-2022-23097	An issue was discovered in the DNS proxy in Connman through 1.40. forward_dns_reply mishandles a strnlen call, leading to an out-of-bounds read.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23096	An issue was discovered in the DNS proxy in Connman through 1.40. The TCP server reply implementation lacks a check for the presence of sufficient Header Data, leading to an out-of-bounds read.	9.1	More Details
CVE-2021-45079	In strongSwan before 5.9.5, a malicious responder can send an EAP-Success message too early without actually authenticating the client and (in the case of EAP methods with mutual authentication and EAP-only authentication for IKEv2) even without server authentication.	9.1	More Details
CVE-2022-21723	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In versions 2.11.1 and prior, parsing an incoming SIP message that contains a malformed multipart can potentially cause out-of-bound read access. This issue affects all PJSIP users that accept SIP multipart. The patch is available as commit in the `master` branch. There are no known workarounds.	9.1	More Details
CVE-2022-24218	An issue in /admin/delete_image.php of eliteCMS v1.0 allows attackers to delete arbitrary files.	9.1	More Details
CVE-2022-21722	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In version 2.11.1 and prior, there are various cases where it is possible that certain incoming RTP/RTCP packets can potentially cause out-of-bound read access. This issue affects all users that use PJMEDIA and accept incoming RTP/RTCP. A patch is available as a commit in the `master` branch. There are no known workarounds.	9.1	More Details
CVE-2022-23959	In Varnish Cache before 6.6.2 and 7.x before 7.0.2, Varnish Cache 6.0 LTS before 6.0.10, and and Varnish Enterprise (Cache Plus) 4.1.x before 4.1.11r6 and 6.0.x before 6.0.9r4, request smuggling can occur for HTTP/1 connections.	9.1	More Details
CVE-2022-24123	MarkText through 0.16.3 does not sanitize the input of a mermaid block before rendering. This could lead to Remote Code Execution via a .md file containing a mutation Cross-Site Scripting (XSS) payload.	9.0	More Details
CVE-2022-21686	PrestaShop is an Open Source e-commerce platform. Starting with version 1.7.0.0 and ending with version 1.7.8.3, an attacker is able to inject twig code inside the back office when using the legacy layout. The problem is fixed in version 1.7.8.3. There are no known workarounds.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-40416	An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of reolink RLC-410W v3.0.0.136_20121102. All the Get APIs that are not included in cgi_check_ability are already executable by any logged-in users. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2021-44123	SPIP 4.0.0 is affected by a remote command execution vulnerability. To exploit the vulnerability, an attacker must craft a malicious picture with a double extension, upload it and then click on it to execute it.	8.8	More Details
CVE-2021-32849	Gerapy is a distributed crawler management framework. Prior to version 0.9.9, an authenticated user could execute arbitrary commands. This issue is fixed in version 0.9.9. There are no known workarounds.	8.8	More Details
CVE-2021-46097	Dolphinphp v1.5.0 contains a remote code execution vulnerability in /application/common.php#action_log	8.8	More Details
CVE-2021-45897	SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows remote code execution.	8.8	More Details
CVE-2021-22724	A CVE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could allow an attacker to impersonate the user or carry out actions on their behalf when crafted malicious parameters are submitted in POST requests sent to the charging station web server. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	8.8	More Details
CVE-2021-22725	A CVE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could allow an attacker to impersonate the user or carry out actions on their behalf when crafted malicious parameters are submitted in POST requests sent to the charging station web server. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	8.8	More Details
CVE-2021-22826	A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the user visits a page containing the injected payload. This CVE is unique from CVE-2021-22827. Affected Product: EcoStruxure Power Monitoring Expert 9.0 and prior versions	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22827	A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the user visits a page containing the injected payload. This CVE is unique from CVE-2021-22826. Affected Product: EcoStruxure Power Monitoring Expert 9.0 and prior versions	8.8	More Details
CVE-2021-40388	A privilege escalation vulnerability exists in Advantech SQ Manager Server 1.0.6. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-40389	A privilege escalation vulnerability exists in the installation of Advantech DeviceOn/iEdge Server 1.0.2. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-40396	A privilege escalation vulnerability exists in the installation of Advantech DeviceOn/iService 1.1.7. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2021-29845	IBM Security Guardium Insights 3.0 could allow an authenticated user to perform unauthorized actions due to improper input validation. IBM X-Force ID: 205255.	8.8	More Details
CVE-2022-0355	Improper Removal of Sensitive Information Before Storage or Transfer in NPM simple-get prior to 4.0.1.	8.8	More Details
CVE-2021-44122	SPIP 4.0.0 is affected by a Cross Site Request Forgery (CSRF) vulnerability in ecrire/public/aiguiller.php, ecrire/public/balises.php, ecrire/balise/formulaire_.php. To exploit the vulnerability, a visitor must visit a malicious website which redirects to the SPIP website. It is also possible to combine XSS vulnerabilities in SPIP 4.0.0 to exploit it. The vulnerability allows an authenticated attacker to execute malicious code without the knowledge of the user on the website (CSRF).	8.8	More Details
CVE-2022-22994	A remote code execution vulnerability was discovered on Western Digital My Cloud devices where an attacker could trick a NAS device into loading through an unsecured HTTP call. This was a result insufficient verification of calls to the device. The vulnerability was addressed by disabling checks for internet connectivity using HTTP.	8.8	More Details
CVE-2022-23888	YzmCMS v6.3 was discovered to contain a Cross-Site Request Forgey (CSRF) via the component /yzmcms/comment/index/init.html.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24763	The Perfect Survey WordPress plugin before 1.5.2 does not have proper authorisation nor CSRF checks in the save_global_setting AJAX action, allowing unauthenticated users to edit surveys and modify settings. Given the lack of sanitisation and escaping in the settings, this could also lead to a Stored Cross-Site Scripting issue which will be executed in the context of a user viewing any survey	8.8	More Details
CVE-2021-24919	The Wicked Folders WordPress plugin before 2.8.10 does not sanitise and escape the folder_id parameter before using it in a SQL statement in the wicked_folders_save_sort_order AJAX action, available to any authenticated user. leading to an SQL injection	8.8	More Details
CVE-2021-46114	jpress v 4.2.0 is vulnerable to RCE via io.jpress.module.product.ProductNotifyKit#doSendEmail. The admin panel provides a function through which attackers can edit the email templates and inject some malicious code.	8.8	More Details
CVE-2021-22821	A CWE-918 Server-Side Request Forgery (SSRF) vulnerability exists that could cause the station web server to forward requests to unintended network targets when crafted malicious parameters are submitted to the charging station web server. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	8.6	More Details
CVE-2021-44793	Single Connect does not perform an authorization check when using the sc-reports-ui" module. A remote attacker could exploit this vulnerability to access the device configuration page and export the data to an external file. The exploitation of this vulnerability might allow a remote attacker to obtain sensitive information including the database credentials. Since the database runs with high privileges it is possible to execute commands with the attained credentials.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23597	Element Desktop is a Matrix client for desktop platforms with Element Web at its core. Element Desktop before 1.9.7 is vulnerable to a remote program execution bug with user interaction. The exploit is non-trivial and requires clicking on a malicious link, followed by another button click. To the best of our knowledge, the vulnerability has never been exploited in the wild. If you are using Element Desktop < 1.9.7, we recommend upgrading at your earliest convenience. If successfully exploited, the vulnerability allows an attacker to specify a file path of a binary on the victim's computer which then gets executed. Notably, the attacker does *not* have the ability to specify program arguments. However, in certain unspecified configurations, the attacker may be able to specify an URI instead of a file path which then gets handled using standard platform mechanisms. These may allow exploiting further vulnerabilities in those mechanisms, potentially leading to arbitrary code execution.	8.3	More Details
CVE-2022-21796	A memory corruption vulnerability exists in the netserver parse_command_list functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to an out-of-bounds write. An attacker can send an HTTP request to trigger this vulnerability.	8.2	More Details
CVE-2021-44463	Missing DLLs, if replaced by an insider, could allow an attacker to achieve local privilege escalation on the DeltaV Distributed Control System Controllers and Workstations (All versions) when some DeltaV services are started.	8.1	More Details
CVE-2021-42631	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below deserializes attacker controlled leading to pre-auth remote code execution.	8.1	More Details
CVE-2021-42635	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below use a hardcoded APP_KEY value, leading to pre-auth remote code execution.	8.1	More Details
CVE-2016-3735	Piwigo is image gallery software written in PHP. When a criteria is not met on a host, piwigo defaults to usingmt_rand in order to generate password reset tokens. mt_rand output can be predicted after recovering the seed used to generate it. This low an unauthenticated attacker to take over an account providing they know an administrators email address in order to be able to request password reset.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23601	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony form component provides a CSRF protection mechanism by using a random token injected in the form and using the session to store and control the token submitted by the user. When using the FrameworkBundle, this protection can be enabled or disabled with the configuration. If the configuration is not specified, by default, the mechanism is enabled as long as the session is enabled. In a recent change in the way the configuration is loaded, the default behavior has been dropped and, as a result, the CSRF protection is not enabled in form when not explicitly enabled, which makes the application sensible to CSRF attacks. This issue has been resolved in the patch versions listed and users are advised to update. There are no known workarounds for this issue.	8.1	More Details
CVE-2021-42638	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below do not sanitize user input resulting in pre-auth remote code execution.	8.1	More Details
CVE-2021-41766	Apache Karaf allows monitoring of applications and the Java runtime by using the Java Management Extensions (JMX). JMX is a Java RMI based technology that relies on Java serialized objects for client server communication. Whereas the default JMX implementation is hardened against unauthenticated deserialization attacks, the implementation used by Apache Karaf is not protected against this kind of attack. The impact of Java deserialization vulnerabilities strongly depends on the classes that are available within the targets class path. Generally speaking, deserialization of untrusted data does always represent a high security risk and should be prevented. The risk is low as, by default, Karaf uses a limited set of classes in the JMX server class path. It depends of system scoped classes (e.g. jar in the lib folder).	8.1	More Details
CVE-2021-22825	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could allow an attacker to access the system with elevated privileges when a privileged account clicks on a malicious URL that compromises the security token. Affected Products: AP7xxxx and AP8xxx with NMC2 (V6.9.6 or earlier), AP7xxx and AP8xxx with NMC3 (V1.1.0.3 or earlier), and APDU9xxx with NMC3 (V1.0.0.28 or earlier)	8.0	More Details
CVE-2022-0359	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-46520	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via mjs_jprintf at src/mjs_util.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23727	There is a privilege escalation vulnerability in some webOS TVs. Due to wrong setting environments, local attacker is able to perform specific operation to exploit this vulnerability. Exploitation may cause the attacker to obtain a higher privilege	7.8	More Details
CVE-2022-22993	A limited SSRF vulnerability was discovered on Western Digital My Cloud devices that could allow an attacker to impersonate a server and reach any page on the server by bypassing access controls. The vulnerability was addressed by creating a whitelist for valid parameters.	7.8	More Details
CVE-2022-22992	A command injection remote code execution vulnerability was discovered on Western Digital My Cloud Devices that could allow an attacker to execute arbitrary system commands on the device. The vulnerability was addressed by escaping individual arguments to shell functions coming from user input.	7.8	More Details
CVE-2021-46518	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via mjs_disown at src/mjs_core.c.	7.8	More Details
CVE-2022-0413	Use After Free in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-27971	Alps Alpine Touchpad Driver 10.3201.101.215 is vulnerable to DLL Injection.	7.8	More Details
CVE-2021-4034	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.	7.8	More Details
CVE-2021-40397	A privilege escalation vulnerability exists in the installation of Advantech WISE-PaaS/OTA Server 3.0.9. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46522	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via /usr/lib/x86_64-linux-gnu/libasan.so.4+0xaff53.	7.8	More Details
CVE-2022-0361	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-46513	Cesanta MJS v2.20.0 was discovered to contain a global buffer overflow via mjs_mk_string at mjs/src/mjs_string.c.	7.8	More Details
CVE-2022-21944	A UNIX Symbolic Link (Symlink) Following vulnerability in the systemd service file for watchman of openSUSE Backports SLE-15-SP3, Factory allows local attackers to escalate to root. This issue affects: openSUSE Backports SLE-15-SP3 watchman versions prior to 4.9.0. openSUSE Factory watchman versions prior to 4.9.0-9.1.	7.8	More Details
CVE-2021-27654	Forgotten password reset functionality for local accounts can be used to bypass local authentication checks.	7.8	More Details
CVE-2021-45975	In ListCheck.exe in Acer Care Center 4.x before 4.00.3038, a vulnerability in the loading mechanism of Windows DLLs could allow a local attacker to perform a DLL hijacking attack. This vulnerability is due to incorrect handling of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with local administrator privileges.	7.8	More Details
CVE-2021-46509	Cesanta MJS v2.20.0 was discovered to contain a stack overflow via snquote at mjs/src/mjs_json.c.	7.8	More Details
CVE-2021-22808	A CWE-416: Use After Free vulnerability exists that could cause arbitrary code execution when a malicious *.gd1 configuration file is loaded into the GUIcon tool. Affected Product: Eurotherm by Schneider Electric GUIcon Version 2.0 (Build 683.003) and prior	7.8	More Details
CVE-2021-46521	Cesanta MJS v2.20.0 was discovered to contain a global buffer overflow via c_vsnprintf at mjs/src/common/str_util.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46519	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via mjs_array_length at src/mjs_array.c.	7.8	More Details
CVE-2021-46523	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via to_json_or_debug at mjs/src/mjs_json.c.	7.8	More Details
CVE-2022-0407	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-0368	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-0392	Heap-based Buffer Overflow in GitHub repository vim prior to 8.2.	7.8	More Details
CVE-2021-46524	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via snquote at mjs/src/mjs_json.c.	7.8	More Details
CVE-2022-24122	kernel/ucount.c in the Linux kernel 5.14 through 5.16.4, when unprivileged user namespaces are enabled, allows a use-after-free and privilege escalation because a ucounts object can outlive its namespace.	7.8	More Details
CVE-2022-0417	Heap-based Buffer Overflow GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-22807	A CWE-787: Out-of-bounds Write vulnerability exists that could cause arbitrary code execution when a malicious *.gd1 configuration file is loaded into the GUIcon tool. Affected Product: Eurotherm by Schneider Electric GUIcon Version 2.0 (Build 683.003) and prior	7.8	More Details
CVE-2022-0408	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-46526	Cesanta MJS v2.20.0 was discovered to contain a global buffer overflow via snquote at src/mjs_json.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46527	Cesanta MJS v2.20.0 was discovered to contain a heap buffer overflow via mjs_get_cstring at src/mjs_string.c.	7.8	More Details
CVE-2021-46525	Cesanta MJS v2.20.0 was discovered to contain a heap-use-after-free via mjs_apply at src/mjs_exec.c.	7.8	More Details
CVE-2021-44415	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. ModifyUser param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44399	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetPtzPreset param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44400	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetPtzPatrol param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44414	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. DelUser param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44401	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. PtzCtrl param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44413	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. AddUser param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44402	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetPtzSerial param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44412	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetRec param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44407	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. TestEmail param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44403	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetPtzTattern param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44404	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetZoomFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44411	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Search param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44398	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. rtmp=stop param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44405	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. StartZoomFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44378	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetEnc param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44406	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetAutoFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44408	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. TestFtp param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44410	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. UpgradePrepare param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44409	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. TestWifi param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44397	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. rtmp=start param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44358	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetRec param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44360	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetNorm param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44361	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Set3G param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44362	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetCloudSchedule param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44363	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetPush param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44364	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetWifi param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44365	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetDevName param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44367	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetUpnp param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44368	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetNetPort param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44369	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetNtp param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44370	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetFtp param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44371	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetEmail param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44372	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetLocalLink param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44373	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetAutoFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44374	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetMask param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44376	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetIsp param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44359	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetCrop param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44379	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetAutoMaint param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44396	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Preview param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44380	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetTime param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44395	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetMask param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44393	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetIsp param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44417	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetAlarm param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44392	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetImage param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44391	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetEnc param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44390	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Format param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44389	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetAbility param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44388	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Login param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44387	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetPtzPreset param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44386	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetPtzPatrol param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44385	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetPtzSerial param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44384	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetPtzTattern param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44383	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetAutoUpgrade param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44382	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot.SetIrLights param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44381	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetPowerLed param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44416	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Disconnect param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44377	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. SetImage param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2021-44418	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetMdState param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details
CVE-2022-23602	Nimforum is a lightweight alternative to Discourse written in Nim. In versions prior to 2.2.0 any forum user can create a new thread/post with an include referencing a file local to the host operating system. Nimforum will render the file if able. This can also be done silently by using NimForum's post "preview" endpoint. Even if NimForum is running as a non-critical user, the forum.json secrets can be stolen. Version 2.2.0 of NimForum includes patches for this vulnerability. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue.	7.7	More Details
CVE-2021-44419	A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetMdAlarm param is not object. An attacker can send an HTTP request to trigger this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40406	A denial of service vulnerability exists in the cgiserver.cgi session creation functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to prevent users from logging in. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2022-24266	Cuppa CMS v1.0 was discovered to contain a SQL injection vulnerability in /administrator/components/table_manager/ via the order_by parameter.	7.5	More Details
CVE-2021-46669	MariaDB through 10.5.9 allows attackers to trigger a convert_const_to_int use-after-free when the BIGINT data type is used.	7.5	More Details
CVE-2021-22816	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a Denial of Service of the RTU when receiving a specially crafted request over Modbus, and the RTU is configured as a Modbus server. Affected Products: SCADAPack 312E, 313E, 314E, 330E, 333E, 334E, 337E, 350E and 357E RTUs with firmware V8.18.1 and prior	7.5	More Details
CVE-2021-22818	A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to gain unauthorized access to the charging station web interface by performing brute force attacks. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	7.5	More Details
CVE-2021-41040	In Eclipse Wakaama, ever since its inception until 2021-01-14, the CoAP parsing code does not properly sanitize network-received data.	7.5	More Details
CVE-2021-43859	XStream is an open source java library to serialize objects to XML and back again. Versions prior to 1.4.19 may allow a remote attacker to allocate 100% CPU time on the target system depending on CPU type or parallel execution of such a payload resulting in a denial of service only by manipulating the processed input stream. XStream 1.4.19 monitors and accumulates the time it takes to add elements to collections and throws an exception if a set threshold is exceeded. Users are advised to upgrade as soon as possible. Users unable to upgrade may set the NO_REFERENCE mode to prevent recursion. See GHSA-rmr5-cpv2-vgjf for further details on a workaround if an upgrade is not possible.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23596	Junrar is an open source java RAR archive library. In affected versions A carefully crafted RAR archive can trigger an infinite loop while extracting said archive. The impact depends solely on how the application uses the library, and whether files can be provided by malignant users. The problem is patched in 7.4.1. There are no known workarounds and users are advised to upgrade as soon as possible.	7.5	More Details
CVE-2022-23968	Xerox VersaLink devices on specific versions of firmware before 2022-01-26 allow remote attackers to brick the device via a crafted TIFF file in an unauthenticated HTTP POST request. There is a permanent denial of service because image parsing causes a reboot, but image parsing is restarted as soon as the boot process finishes. However, this boot loop can be resolved by a field technician. The TIFF file must have an incomplete Image Directory. Affected firmware versions include xx.42.01 and xx.50.61. NOTE: the 2022-01-24 NeoSmart article included "believed to affect all previous and later versions as of the date of this posting" but a 2022-01-26 vendor statement reports "the latest versions of firmware are not vulnerable to this issue."	7.5	More Details
CVE-2021-40419	A firmware update vulnerability exists in the 'factory' binary of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted series of network requests can lead to arbitrary firmware update. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details
CVE-2022-24264	Cuppa CMS v1.0 was discovered to contain a SQL injection vulnerability in /administrator/components/table_manager/ via the search_word parameter.	7.5	More Details
CVE-2021-40423	A denial of service vulnerability exists in the cgiserver.cgi API command parser functionality of Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted series of HTTP requests can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2021-46102	From version 0.2.14 to 0.2.16 for Solana rBPF, function "relocate" in the file src/elf.rs has an integer overflow bug because the sym.st_value is read directly from ELF file without checking. If the sym.st_value is rather large, an integer overflow is triggered while calculating the variable "addr" via "addr = (sym.st_value + refd_pa) as u64";	7.5	More Details
CVE-2022-21134	A firmware update vulnerability exists in the "update" firmware checks functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to firmware update. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21236	An information disclosure vulnerability exists due to a web server misconfiguration in the Reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a disclosure of sensitive information. An attacker can send an HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2022-21801	A denial of service vulnerability exists in the netserver recv_command functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted network request can lead to a reboot. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2021-46383	https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: SQL Injection. The impact is: obtain sensitive information (remote). The component is: net.mingsoft.mdiy.action.web.DictAction#list. The attack vector is: 0 or sleep(3). ¶¶ MCMS has a sql injection vulnerability through which attacker can get sensitive information from the database.	7.5	More Details
CVE-2021-25093	The Link Library WordPress plugin before 7.2.8 does not have authorisation in place when deleting links, allowing unauthenticated users to delete arbitrary links via a crafted request	7.5	More Details
CVE-2022-22828	An insecure direct object reference for the file-download URL in Synametrics SynaMan before 5.0 allows a remote attacker to access unshared files via a modified base64-encoded filename string.	7.5	More Details
CVE-2022-23990	Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function.	7.5	More Details
CVE-2021-46385	https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: SQL Injection. The impact is: obtain sensitive information (remote). The component is: net.mingsoft.mdiy.action.FormDataAction#queryData. The attack vector is: 0 or sleep(3). ¶¶ MCMS has a sql injection vulnerability through which attacker can get sensitive information from the database.	7.5	More Details
CVE-2022-24265	Cuppa CMS v1.0 was discovered to contain a SQL injection vulnerability in /administrator/components/menu/ via the path=component/menu/&menu_filter=3 parameter.	7.5	More Details
CVE-2021-46559	The firmware on Moxa TN-5900 devices through 3.1 has a weak algorithm that allows an attacker to defeat an inspection mechanism for integrity protection.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34805	An issue was discovered in FAUST iServer before 9.0.019.019.7. For each URL request, it accesses the corresponding .fau file on the operating system without preventing %2e%2e%5c directory traversal.	7.5	More Details
CVE-2021-46101	In Git for windows through 2.34.1 when using git pull to update the local warehouse, git.cmd can be run directly.	7.5	More Details
CVE-2022-23098	An issue was discovered in the DNS proxy in Connman through 1.40. The TCP server reply implementation has an infinite loop if no data is received.	7.5	More Details
CVE-2021-46459	Victor CMS v1.0 was discovered to contain multiple SQL injection vulnerabilities in the component admin/users.php?source=add_user. These vulnerabilities can be exploited through a crafted POST request via the user_name, user_firstname,user_lastname, or user_email parameters.	7.5	More Details
CVE-2022-24124	The query API in Casdoor before 1.13.1 has a SQL injection vulnerability related to the field and value parameters, as demonstrated by api/get-organizations.	7.5	More Details
CVE-2021-46458	Victor CMS v1.0 was discovered to contain a SQL injection vulnerability in the component admin/posts.php?source=add_post. This vulnerability can be exploited through a crafted POST request via the post_title parameter.	7.5	More Details
CVE-2021-41608	A file disclosure vulnerability in the UploadedImageDisplay.aspx endpoint of SelectSurvey.NET before 5.052.000 allows a remote, unauthenticated attacker to retrieve survey user submitted data by modifying the value of the ID parameter in sequential order beginning from 1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43848	h2o is an open source http server. In code prior to the `8c0eca3` commit h2o may attempt to access uninitialized memory. When receiving QUIC frames in certain order, HTTP/3 server-side implementation of h2o can be misguided to treat uninitialized memory as HTTP/3 frames that have been received. When h2o is used as a reverse proxy, an attacker can abuse this vulnerability to send internal state of h2o to backend servers controlled by the attacker or third party. Also, if there is an HTTP endpoint that reflects the traffic sent from the client, an attacker can use that reflector to obtain internal state of h2o. This internal state includes traffic of other connections in unencrypted form and TLS session tickets. This vulnerability exists in h2o server with HTTP/3 support, between commit 93af138 and d1f0f65. None of the released versions of h2o are affected by this vulnerability. There are no known workarounds. Users of unreleased versions of h2o using HTTP/3 are advised to upgrade immediately.	7.4	More Details
CVE-2021-23558	The package bmoor before 0.10.1 are vulnerable to Prototype Pollution due to missing sanitization in set function. **Note:** This vulnerability derives from an incomplete fix in [CVE-2020-7736] (https://security.snyk.io/vuln/SNYK-JS-BMOOR-598664)	7.3	More Details
CVE-2021-42791	An issue was discovered in VeridiumID VeridiumAD 2.5.3.0. The HTTP request to trigger push notifications for VeridiumAD enrolled users does not enforce proper access control. A user can trigger push notifications for any other user. The text contained in the push notification can also be modified. If a user who receives the notification accepts it, then the user who triggered the notification can obtain the accepting user's login certificate.	7.3	More Details
CVE-2021-32840	SharpZipLib (or #ziplib) is a Zip, GZip, Tar and BZip2 library. Prior to version 1.3.3, a TAR file entry `../evil.txt` may be extracted in the parent directory of `destFolder`. This leads to arbitrary file write that may lead to code execution. The vulnerability was patched in version 1.3.3.	7.3	More Details
CVE-2021-46118	jpress 4.2.0 is vulnerable to remote code execution via io.jpress.module.article.kit.ArticleNotifyKit#doSendEmail. The admin panel provides a function through which attackers can edit the email templates and inject some malicious code.	7.2	More Details
CVE-2020-28884	Liferay Portal Server tested on 7.3.5 GA6, 7.2.0 GA1 is affected by OS Command Injection. An administrator user can inject Groovy script to execute any OS command on the Liferay Portal Sever. NOTE: The developer disputes this as a vulnerability since it is a feature for administrators to run groovy scripts and therefore not a design flaw.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40410	An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [4] the dns_data->dns1 variable, that has the value of the dns1 parameter provided through the SetLocal API, is not validated properly. This would lead to an OS command injection.	7.2	More Details
CVE-2021-40411	An OS command injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [6] the dns_data->dns2 variable, that has the value of the dns2 parameter provided through the SetLocalLink API, is not validated properly. This would lead to an OS command injection.	7.2	More Details
CVE-2021-40412	An OScommand injection vulnerability exists in the device network settings functionality of reolink RLC-410W v3.0.0.136_20121102. At [8] the devname variable, that has the value of the name parameter provided through the SetDevName API, is not validated properly. This would lead to an OS command injection.	7.2	More Details
CVE-2021-46088	Zabbix 4.0 LTS, 4.2, 4.4, and 5.0 LTS is vulnerable to Remote Code Execution (RCE). Any user with the "Zabbix Admin" role is able to run custom shell script on the application server in the context of the application user.	7.2	More Details
CVE-2021-44255	Authenticated remote code execution in MotionEye <= 0.42.1 and MotioneEyeOS <= 20200606 allows a remote attacker to upload a configuration backup file containing a malicious python pickle file which will execute arbitrary code on the server.	7.2	More Details
CVE-2021-46561	controller/org.controller/org.controller.js in the CVE Services API 1.1.1 before 5c50baf3bda28133a3bc90b854765a64fb538304 allows an organizational administrator to transfer a user account to an arbitrary new organization, and thereby achieve unintended access within the context of that new organization.	7.2	More Details
CVE-2021-46115	jpress 4.2.0 is vulnerable to RCE via io.jpress.web.admin._TemplateController#doUploadFile. The admin panel provides a function through which attackers can upload templates and inject some malicious code.	7.2	More Details
CVE-2021-46116	jpress 4.2.0 is vulnerable to remote code execution via io.jpress.web.admin._TemplateController#doInstall. The admin panel provides a function through which attackers can install templates and inject some malicious code.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28885	Liferay Portal Server tested on 7.3.5 GA6, 7.2.0 GA1 is affected by OS Command Injection. An administrator user can inject commands through the Gogo Shell module to execute any OS command on the Liferay Portal Sever. NOTE: The developer disputes this as a vulnerability since it is a feature for administrators to access and execute commands in Gogo Shell and therefore not a design fla	7.2	More Details
CVE-2021-46117	jpress 4.2.0 is vulnerable to remote code execution via io.jpress.module.page.PageNotifyKit#doSendEmail. The admin panel provides a function through which attackers can edit the email templates and inject some malicious code.	7.2	More Details
CVE-2021-28962	Stormshield Network Security (SNS) before 4.2.2 allows a read-only administrator to gain privileges via CLI commands.	7.2	More Details
CVE-2021-40413	An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of reolink RLC-410W v3.0.0.136_20121102. The UpgradePrepare is the API that checks if a provided filename identifies a new version of the RLC-410W firmware. If the version is new, it would be possible, allegedly, to later on perform the Upgrade. An attacker can send an HTTP request to trigger this vulnerability.	7.1	More Details
CVE-2022-0393	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.	7.1	More Details
CVE-2021-40414	An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of reolink RLC-410W v3.0.0.136_20121102. The SetMdAlarm API sets the movement detection parameters, giving the ability to set the sensitivity of the camera per a range of hours, and which of the camera spaces to ignore when considering movement detection. Because in cgi_check_ability the SetMdAlarm API does not have a specific case, the user permission will default to 7. This will give non-administrative users the possibility to change the movement detection parameters.	7.1	More Details
CVE-2022-23181	The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8.5.73 that allowed a local attacker to perform actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31567	Authenticated (admin+) Arbitrary File Download vulnerability discovered in Download Monitor WordPress plugin (versions <= 4.4.6). The plugin allows arbitrary files, including sensitive configuration files such as wp-config.php, to be downloaded via the &downloadable_file_urls[0] parameter data. It's also possible to escape from the web server home directory and download any file within the OS.	6.8	More Details
CVE-2022-21687	gh-ost is a triggerless online schema migration solution for MySQL. Versions prior to 1.1.3 are subject to an arbitrary file read vulnerability. The attacker must have access to the target host or trick an administrator into executing a malicious gh-ost command on a host running gh-ost, plus network access from host running gh-ost to the attack's malicious MySQL server. The `-database` parameter does not properly sanitize user input which can lead to arbitrary file reads.	6.8	More Details
CVE-2022-22791	SYNEL - eharmony Authenticated Blind & Stored XSS. Inject JS code into the "comments" field could lead to potential stealing of cookies, loading of HTML tags and JS code onto the system.	6.6	More Details
CVE-2021-22600	A double free bug in packet_set_ring() in net/packet/af_packet.c can be exploited by a local user through crafted syscalls to escalate privileges or deny service. We recommend upgrading kernel past the effected versions or rebuilding past ec6af094ea28f0f2dda1a6a33b14cd57e36a9755	6.6	More Details
CVE-2022-0273	Improper Access Control in Pypi calibreweb prior to 0.6.16.	6.5	More Details
CVE-2022-23863	Zoho ManageEngine Desktop Central before 10.1.2137.10 allows an authenticated user to change any user's login password.	6.5	More Details
CVE-2021-25072	The NextScripts: Social Networks Auto-Poster WordPress plugin before 4.3.25 does not have CSRF check in place when deleting items, allowing attacker to make a logged in admin delete arbitrary posts via a CSRF attack	6.5	More Details
CVE-2022-22938	VMware Workstation (16.x prior to 16.2.2) and Horizon Client for Windows (5.x prior to 5.5.3) contains a denial-of-service vulnerability in the Cortado ThinPrint component. The issue exists in TrueType font parser. A malicious actor with access to a virtual machine or remote desktop may exploit this issue to trigger a denial-of-service condition in the Thinprint service running on the host machine where VMware Workstation or Horizon Client for Windows is installed.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25097	The LabTools WordPress plugin through 1.0 does not have proper authorisation and CSRF check in place when deleting publications, allowing any authenticated users, such as subscriber to delete arbitrary publication	6.5	More Details
CVE-2021-25092	The Link Library WordPress plugin before 7.2.8 does not have CSRF check when resetting library settings, allowing attackers to make a logged in admin reset arbitrary settings via a CSRF attack	6.5	More Details
CVE-2022-23887	YzmCMS v6.3 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily delete user accounts via /admin/admin_manage/delete.	6.5	More Details
CVE-2021-40042	There is a release of invalid pointer vulnerability in some Huawei products, successful exploit may cause the process and service abnormal. Affected product versions include: CloudEngine 12800 V200R019C10SPC800, V200R019C10SPC900; CloudEngine 5800 V200R019C10SPC800, V200R020C00SPC600; CloudEngine 6800 versions V200R019C10SPC800, V200R019C10SPC900, V200R020C00SPC600, V300R020C00SPC200; CloudEngine 7800 V200R019C10SPC800.	6.5	More Details
CVE-2021-41571	In Apache Pulsar it is possible to access data from BookKeeper that does not belong to the topics accessible by the authenticated user. The Admin API get-message-by-id requires the user to input a topic and a ledger id. The ledger id is a pointer to the data, and it is supposed to be a valid it for the topic. Authorisation controls are performed against the topic name and there is not proper validation the that ledger id is valid in the context of such ledger. So it may happen that the user is able to read from a ledger that contains data owned by another tenant. This issue affects Apache Pulsar Apache Pulsar version 2.8.0 and prior versions; Apache Pulsar version 2.7.3 and prior versions; Apache Pulsar version 2.6.4 and prior versions.	6.5	More Details
CVE-2021-44451	Apache Superset up to and including 1.3.2 allowed for registered database connections password leak for authenticated users. This information could be accessed in a non-trivial way. Users should upgrade to Apache Superset 1.4.0 or higher.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23607	treq is an HTTP library inspired by requests but written on top of Twisted's Agents. Treq's request methods (`treq.get`, `treq.post`, etc.) and `treq.client.HTTPClient` constructor accept cookies as a dictionary. Such cookies are not bound to a single domain, and are therefore sent to *every* domain ("supercookies"). This can potentially cause sensitive information to leak upon an HTTP redirect to a different domain., e.g. should `https://example.com` redirect to `http://cloudstorageprovider.com` the latter will receive the cookie `session`. Treq 2021.1.0 and later bind cookies given to request methods (`treq.request`, `treq.get`, `HTTPClient.request`, `HTTPClient.get`, etc.) to the origin of the *url* parameter. Users are advised to upgrade. For users unable to upgrade Instead of passing a dictionary as the *cookies* argument, pass a `http.cookiejar.CookieJar` instance with properly domain- and scheme-scoped cookies in it.	6.5	More Details
CVE-2021-22570	Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.	6.5	More Details
CVE-2022-24196	iText v7.1.17, up to (exluding)": 7.1.18 and 7.2.2 was discovered to contain an out-of-memory error via the component readStreamBytesRaw, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.	6.5	More Details
CVE-2021-24761	The Error Log Viewer WordPress plugin before 1.1.2 does not perform nonce check when deleting a log file and does not have path traversal prevention, which could allow attackers to make a logged in admin delete arbitrary text files on the web server.	6.5	More Details
CVE-2021-40415	An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of reolink RLC-410W v3.0.0.136_20121102. In cgi_check_ability the Format API does not have a specific case, the user permission will default to 7. This will give non-administrative users the possibility to format the SD card and reboot the device.	6.5	More Details
CVE-2022-24198	iText v7.1.17 was discovered to contain an out-of-bounds exception via the component ARCFOUREncryption.encryptARCFOUR, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file. NOTE: Vendor does not view this as a vulnerability and has not found it to be exploitable.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24197	iText v7.1.17 was discovered to contain a stack-based buffer overflow via the component ByteBuffer.append, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.	6.5	More Details
CVE-2021-40404	An authentication bypass vulnerability exists in the cgiserver.cgi Login functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to authentication bypass. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2021-38560	Ivanti Service Manager 2021.1 allows reflected XSS via the appName parameter associated with ConfigDB calls, such as in RelocateAttachments.aspx.	6.1	More Details
CVE-2021-22811	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause script execution when the request of a privileged account accessing the vulnerable web page is intercepted. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10,	6.1	More Details

CVE Number	Description	Base Score	Reference
	PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)		
	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to a delete policy file. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2		

CVE Number	Description	Base Score	Reference
	AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power		
CVE-2021-22810	Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)	6.1	More Details
CVE-2021-45416	Reflected Cross-site scripting (XSS) vulnerability in RosarioSIS 8.2.1 allows attackers to inject arbitrary HTML via the search_term parameter in the modules/Scheduling/Courses.php script.	6.1	More Details
	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists which could cause arbitrary script execution when a malicious file is read and displayed. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J,		

CVE Number	Description	Base Score	Reference
	AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P),		
CVE-2021-22814	Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)	6.1	More Details
	A CWE-79: Improper Neutralization of Input During Web Page Generation		

CVE Number	Description	Base Score	Reference
	('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair		
CVE-2021-22812		6.1	More Details

CVE Number	Description	Base Score	Reference
	IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)		
CVE-2022-0220	The check_privacy_settings AJAX action of the WordPress GDPR WordPress plugin before 1.9.27, available to both unauthenticated and authenticated users, responds with JSON data without an "application/json" content-type. Since an HTML payload isn't properly escaped, it may be interpreted by a web browser led to this endpoint. Javascript code may be executed on a victim's browser. Due to v1.9.26 adding a CSRF check, the XSS is only exploitable against unauthenticated users (as they all share the same nonce)	6.1	More Details
CVE-2022-0352	Cross-site Scripting (XSS) - Reflected in Pypi calibreweb prior to 0.6.16.	6.1	More Details
CVE-2022-23993	/usr/local/www/pkg.php in pfSense CE before 2.6.0 and pfSense Plus before 22.01 uses $_REQUEST['pkg_filter'] in a PHP echo call, causing XSS.	6.1	More Details
	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to an edit policy file. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using		

CVE Number	Description	Base Score	Reference
CVE-2021-22813	NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)	6.1	More Details
CVE-2021-24764	The Perfect Survey WordPress plugin before 1.5.2 does not sanitise and escape multiple parameters (id and filters[session_id] of single_statistics page, type and message of importexport page) before outputting them back in pages/attributes in the admin dashboard, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2021-25085	The WOOF WordPress plugin before 1.2.6.3 does not sanitise and escape the woof_redraw_elements before outputing back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22822	A CWE-79 Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) vulnerability exists that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	6.1	More Details
CVE-2021-25091	The Link Library WordPress plugin before 7.2.9 does not sanitise and escape the settingscopy parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-24934	The Visual CSS Style Editor WordPress plugin before 7.5.4 does not sanitise and escape the wyp_page_type parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-24937	The Asset CleanUp: Page Speed Booster WordPress plugin before 1.3.8.5 does not escape the wpacu_selected_sub_tab_area parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-26264	A specially crafted script could cause the DeltaV Distributed Control System Controllers (All Versions) to restart and cause a denial-of-service condition.	6.1	More Details
CVE-2021-23863	HTML code injection vulnerability in Android Application, Bosch Video Security, version 3.2.3. or earlier, when successfully exploited allows an attacker to inject random HTML code into a component loaded by WebView, thus allowing the Application to display web resources controlled by the attacker.	6.1	More Details
CVE-2021-24648	The RegistrationMagic WordPress plugin before 5.0.1.9 does not sanitise and escape the rm_search_value parameter before outputting back in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-24975	The NextScripts: Social Networks Auto-Poster WordPress plugin before 4.3.24 does not sanitise and escape logged requests before outputting them in the related admin dashboard, leading to an Unauthenticated Stored Cross-Site Scripting issue	6.1	More Details
CVE-2021-24926	The Domain Check WordPress plugin before 1.0.17 does not sanitise and escape the domain parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24983	The Asset CleanUp: Page Speed Booster WordPress plugin before 1.3.8.5 does not sanitise and escape POSted parameters sent to the wpassetcleanup_fetch_active_plugins_icons AJAX action (available to admin users), leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-21719	GLPI is a free asset and IT management software package. All GLPI versions prior to 9.5.7 are vulnerable to reflected cross-site scripting. Version 9.5.7 contains a patch for this issue. There are no known workarounds.	6.1	More Details
CVE-2021-25063	The Skins for Contact Form 7 WordPress plugin before 2.5.1 does not sanitise and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-22919	Adenza AxiomSL ControllerView through 10.8.1 allows redirection for SSO login URLs.	6.1	More Details
CVE-2021-24765	The Perfect Survey WordPress plugin through 1.5.2 does not validate and escape the X-Forwarded-For header value before outputting it in the statistic page when the Anonymize IP setting of a survey is turned off, leading to a Stored Cross-Site Scripting issue	6.1	More Details
CVE-2021-25089	The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.16.69 does not sanitise and escape the updraft_restore parameter before outputting it back in the Restore page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-23598	laminas-form is a package for validating and displaying simple and complex forms. When rendering validation error messages via the `formElementErrors()` view helper shipped with laminas-form, many messages will contain the submitted value. However, in laminas-form prior to version 3.1.1, the value was not being escaped for HTML contexts, which could potentially lead to a reflected cross-site scripting attack. Versions 3.1.1 and above contain a patch to mitigate the vulnerability. A workaround is available. One may manually place code at the top of a view script where one calls the `formElementErrors()` view helper. More information about this workaround is available on the GitHub Security Advisory.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4160	There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).	5.9	More Details
CVE-2022-21721	Next.js is a React framework. Starting with version 12.0.0 and prior to version 12.0.9, vulnerable code could allow a bad actor to trigger a denial of service attack for anyone using i18n functionality. In order to be affected by this CVE, one must use next start or a custom server and the built-in i18n support. Deployments on Vercel, along with similar environments where invalid requests are filtered before reaching Next.js, are not affected. A patch has been released, `next@12.0.9`, that mitigates this issue. As a workaround, one may ensure `/${locale}/_next/` is blocked from reaching the Next.js instance until it becomes feasible to upgrade.	5.9	More Details
CVE-2021-29838	IBM Security Guardium Insights 3.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2022-21199	An information disclosure vulnerability exists due to the hardcoded TLS key of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted man-in-the-middle attack can lead to a disclosure of sensitive information. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23760	The package keyget from 0.0.0 are vulnerable to Prototype Pollution via the methods set, push, and at which could allow an attacker to cause a denial of service and may lead to remote code execution. **Note:** This vulnerability derives from an incomplete fix to [CVE-2020-28272] (https://security.snyk.io/vuln/SNYK-JS-KEYGET-1048048)	5.6	More Details
CVE-2022-22790	SYNEL - eharmony Directory Traversal. Directory Traversal - is an attack against a server or a Web application aimed at unauthorized access to the file system. on the "Name" parameter the attacker can return to the root directory and open the host file. The path exposes sensitive files that users upload	5.6	More Details
CVE-2021-46511	There is an Assertion `m->len >= sizeof(v)' failed at src/mjs_core.c in Cesanta MJS v2.20.0.	5.5	More Details
CVE-2021-46662	MariaDB through 10.5.9 allows a set_var.cc application crash via certain uses of an UPDATE statement in conjunction with a nested subquery.	5.5	More Details
CVE-2021-46661	MariaDB through 10.5.9 allows an application crash in find_field_in_tables and find_order_in_list via an unused common table expression (CTE).	5.5	More Details
CVE-2021-46503	Jsish v3.5.0 was discovered to contain a heap-use-after-free via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46504	There is an Assertion 'vp != resPtr' failed at jsiEval.c in Jsish v3.5.0.	5.5	More Details
CVE-2021-46505	Jsish v3.5.0 was discovered to contain a stack overflow via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x5b1e5.	5.5	More Details
CVE-2021-46506	There is an Assertion 'v->d.lval != v' failed at src/jsiValue.c in Jsish v3.5.0.	5.5	More Details
CVE-2021-46507	Jsish v3.5.0 was discovered to contain a stack overflow via Jsi_LogMsg at src/jsiUtils.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0286	A flaw was found in the Linux kernel. A null pointer dereference in bond_ipsec_add_sa() may lead to local denial of service.	5.5	More Details
CVE-2021-46508	There is an Assertion `i < parts_cnt' failed at src/mjs_bcode.c in Cesanta MJS v2.20.0.	5.5	More Details
CVE-2021-46510	There is an Assertion `s < mjs->owned_strings.buf + mjs->owned_strings.len' failed at src/mjs_gc.c in Cesanta MJS v2.20.0.	5.5	More Details
CVE-2021-46514	There is an Assertion 'ppos != NULL && mjs_is_number(*ppos)' failed at src/mjs_core.c in Cesanta MJS v2.20.0.	5.5	More Details
CVE-2021-46512	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_apply at src/mjs_exec.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46664	MariaDB through 10.5.9 allows an application crash in sub_select_postjoin_aggr for a NULL value of aggr.	5.5	More Details
CVE-2021-23521	This affects the package juce-framework/JUCE before 6.1.5. This vulnerability is triggered when a malicious archive is crafted with an entry containing a symbolic link. When extracted, the symbolic link is followed outside of the target dir allowing writing arbitrary files on the target host. In some cases, this can allow an attacker to execute arbitrary code. The vulnerable code is in the ZipFile::uncompressEntry function in juce_ZipFile.cpp and is executed when the archive is extracted upon calling uncompressTo() on a ZipFile object.	5.5	More Details
CVE-2021-23520	The package juce-framework/juce before 6.1.5 are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) via the ZipFile::uncompressEntry function in juce_ZipFile.cpp. This vulnerability is triggered when the archive is extracted upon calling uncompressTo() on a ZipFile object.	5.5	More Details
CVE-2021-46515	There is an Assertion `mjs_stack_size(&mjs->scopes) >= scopes_len' failed at src/mjs_exec.c in Cesanta MJS v2.20.0.	5.5	More Details
CVE-2021-46516	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_stack_size at mjs/src/mjs_core.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24130	xterm through Patch 370, when Sixel support is enabled, allows attackers to trigger a buffer overflow in set_sixel in graphics_sixel.c via crafted text.	5.5	More Details
CVE-2021-46517	There is an Assertion `mjs_stack_size(&mjs->scopes) > 0' failed at src/mjs_exec.c in Cesanta MJS v2.20.0.	5.5	More Details
CVE-2021-46528	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0x5361e. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46529	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0x8814e. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46530	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_execute at src/mjs_exec.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46663	MariaDB through 10.5.13 allows a ha_maria::extra application crash via certain SELECT statements.	5.5	More Details
CVE-2021-46665	MariaDB through 10.5.9 allows a sql_parse.cc application crash because of incorrect used_tables expectations.	5.5	More Details
CVE-2021-46532	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via exec_expr at src/mjs_exec.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46666	MariaDB before 10.6.2 allows an application crash because of mishandling of a pushdown from a HAVING clause to a WHERE clause.	5.5	More Details
CVE-2021-46484	Jsish v3.5.0 was discovered to contain a heap-use-after-free via Jsi_IncrRefCount in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46485	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via Jsi_ValueIsNumber at src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46486	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via jsi_ArraySpliceCmd at src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46487	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via /lib/x86_64-linux-gnu/libc.so.6+0x18e506. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46488	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via jsi_ArrayConcatCmd at src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46489	Jsish v3.5.0 was discovered to contain a heap-use-after-free via Jsi_DecrRefCount in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46490	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via NumberConstructor at src/jsiNumber.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46491	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via Jsi_CommandPkgOpts at src/jsiCmds.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46492	Jsish v3.5.0 was discovered to contain a SEGV vulnerability via Jsi_FunctionInvoke at src/jsiFunc.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46494	Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_ValueLookupBase in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46495	Jsish v3.5.0 was discovered to contain a heap-use-after-free via DeleteTreeValue in src/jsiObj.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46496	Jsish v3.5.0 was discovered to contain a heap-use-after-free via Jsi_ObjFree in src/jsiObj.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46497	Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_UserObjDelete in src/jsiUserObj.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46498	Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_wswebsocketObjFree in src/jsiWebSocket.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46499	Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_ValueCopyMove in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46500	Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_ArgTypeCheck in src/jsiFunc.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46501	Jsish v3.5.0 was discovered to contain a heap-use-after-free via SortSubCmd in src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2022-0419	NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.0.	5.5	More Details
CVE-2021-46502	Jsish v3.5.0 was discovered to contain a heap-use-after-free via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x5166d. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46668	MariaDB through 10.5.9 allows an application crash via certain long SELECT DISTINCT statements that improperly interact with storage-engine resource limitations for temporary data structures.	5.5	More Details
CVE-2021-46667	MariaDB before 10.6.5 has a sql_lex.cc integer overflow, leading to an application crash.	5.5	More Details
CVE-2021-46531	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0x8d28e. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-40033	There is an information exposure vulnerability on several Huawei Products. The vulnerability is due to that the software does not properly protect certain information. Successful exploit could cause information disclosure. Affected product versions include: CloudEngine 12800 V200R005C10SPC800; CloudEngine 5800 V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 V200R005C10SPC800, V200R019C00SPC800.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46659	MariaDB before 10.7.2 allows an application crash because it does not recognize that SELECT_LEX::nest_level is local to each VIEW.	5.5	More Details
CVE-2021-46541	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0x2c6ae. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46554	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_json_stringify at src/mjs_json.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46553	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_set_internal at src/mjs_object.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46550	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via free_json_frame at src/mjs_json.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46549	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via parse_cval_type at src/mjs_ffi.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46548	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via add_lineno_map_item at src/mjs_bcode.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46547	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0x2c17e. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46546	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_next at src/mjs_object.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46545	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /lib/x86_64-linux-gnu/libc.so.6+0x4b44b. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46544	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x59e19. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46543	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /lib/x86_64-linux-gnu/libc.so.6+0x18e810. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23456	Potential arbitrary file deletion vulnerability has been identified in HP Support Assistant software.	5.5	More Details
CVE-2021-46542	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_print at src/mjs_builtin.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46556	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_bcode_insert_offset at src/mjs_bcode.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46658	save_window_function_values in MariaDB before 10.6.3 allows an application crash because of incorrect handling of with_window_func=true for a subquery.	5.5	More Details
CVE-2021-46657	get_sort_by_table in MariaDB before 10.6.2 allows an application crash via certain subquery uses of ORDER BY.	5.5	More Details
CVE-2021-46534	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via getprop_builtin_foreign at src/mjs_exec.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46539	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /lib/x86_64-linux-gnu/libc.so.6+0x45a1f. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-22809	A CWE-125:Out-of-Bounds Read vulnerability exists that could cause unintended data disclosure when a malicious *.gd1 configuration file is loaded into the GUIcon tool. Affected Product: Eurotherm by Schneider Electric GUIcon Version 2.0 (Build 683.003) and prior	5.5	More Details
CVE-2021-46538	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via gc_compact_strings at src/mjs_gc.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46535	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0xe533e. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46540	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_get_mjs at src/mjs_builtin.c. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-46537	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via /usr/local/bin/mjs+0x9a30e. This vulnerability can lead to a Denial of Service (DoS).	5.5	More Details
CVE-2021-34073	A Cross Site Scripting (XSS) vulnerabilty exists in Sourcecodester Gadget Works Online Ordering System in PHP/MySQLi 1.0 via the Category parameter in an add function in category/index.php.	5.4	More Details
CVE-2022-0374	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details
CVE-2021-44118	SPIP 4.0.0 is affected by a Cross Site Scripting (XSS) vulnerability. To exploit the vulnerability, a visitor must browse to a malicious SVG file. The vulnerability allows an authenticated attacker to inject malicious code running on the client side into web pages visited by other users (stored XSS).	5.4	More Details
CVE-2022-0379	Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11.	5.4	More Details
CVE-2022-22851	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodtester Hospital's Patient Records Management System 1.0 via the specialization parameter in doctors.php	5.4	More Details
CVE-2021-44120	SPIP 4.0.0 is affected by a Cross Site Scripting (XSS) vulnerability in ecrire/public/interfaces.php, adding the function safehtml to the vulnerable fields. An editor is able to modify his personal information. If the editor has an article written and available, when a user goes to the public site and wants to read the author's information, the malicious code will be executed. The "Who are you" and "Website Name" fields are vulnerable.	5.4	More Details
CVE-2022-0251	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.2.10.	5.4	More Details
CVE-2022-0394	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0378	Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.	5.4	More Details
CVE-2022-0348	Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.2.	5.4	More Details
CVE-2022-0387	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details
CVE-2021-43334	BuddyBoss Platform through 1.8.0 allows XSS via the Group Name or Group Description field.	5.4	More Details
CVE-2022-0372	Cross-site Scripting (XSS) - Stored in Packagist bytefury/crater prior to 6.0.2.	5.4	More Details
CVE-2022-22850	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodtester Hospital's Patient Records Management System 1.0 via the description parameter in room_types.	5.4	More Details
CVE-2022-0395	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details
CVE-2022-0370	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details
CVE-2021-46253	A cross-site scripting (XSS) vulnerability in the Create Post function of Anchor CMS v0.12.7 allows attackers to execute arbitrary web scripts or HTML.	5.4	More Details
CVE-2022-22852	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodtester Hospital's Patient Records Management System 1.0 via the description parameter in room_list.	5.4	More Details
CVE-2021-46447	A cross-site scripting (XSS) vulnerability in H.H.G Multistore v5.1.0 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the State parameter under the Address Book module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36056	Beetel 777VR1-DI Hardware Version REV.1.01 Firmware Version V01.00.09_55 was discovered to contain a cross-site scripting (XSS) vulnerability via the Ping diagnostic option.	5.4	More Details
CVE-2021-44746	UNIVERGE DT 820 V3.2.7.0 and prior, UNIVERGE DT 830 V5.2.7.0 and prior, UNIVERGE DT 930 V2.4.0.0 and prior, IP Phone Manager V8.9.1 and prior, Data Maintenance Tool for DT900 Series V5.3.0.0 and prior, Data Maintenance Tool for DT800 Series V4.2.0.0 and prior allows a remote attacker who can access to the internal network, the configuration information may be obtained.	5.3	More Details
CVE-2022-0203	Improper Access Control in GitHub repository crater-invoice/crater prior to 6.0.2.	5.3	More Details
CVE-2021-44792	Single Connect does not perform an authorization check when using the "log-monitor" module. A remote attacker could exploit this vulnerability to access the logging interface. The exploitation of this vulnerability might allow a remote attacker to obtain sensitive information.	5.3	More Details
CVE-2021-44794	Single Connect does not perform an authorization check when using the "sc-diagnostic-ui" module. A remote attacker could exploit this vulnerability to access the device information page. The exploitation of this vulnerability might allow a remote attacker to obtain sensitive information.	5.3	More Details
CVE-2021-28096	An issue was discovered in Stormshield SNS before 4.2.3 (when the proxy is used). An attacker can saturate the proxy connection table. This would result in the proxy denying any new connections.	5.3	More Details
CVE-2021-44795	Single Connect does not perform an authorization check when using the "sc-assigned-credential-ui" module. A remote attacker could exploit this vulnerability to modify users permissions. The exploitation of this vulnerability might allow a remote attacker to delete permissions from other users without authenticating.	5.3	More Details
CVE-2021-24775	The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.	5.3	More Details
CVE-2019-25056	In Bromite through 78.0.3904.130, there are adblock rules in the release APK; therefore, probing which resources are blocked and which aren't can identify the application version and defeat the User-Agent protection mechanism.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44692	BuddyBoss Platform through 1.8.0 allows remote attackers to obtain the email address of each user. When creating a new user, it generates a Unique ID for their profile. This UID is their private email address with symbols removed and periods replaced with hyphens. For example. JohnDoe@example.com would become /members/johndoeexample-com and Jo.test@example.com would become /members/jo-testexample-com. The members list is available to everyone and (in a default configuration) often without authentication. It is therefore trivial to collect a list of email addresses.	5.3	More Details
CVE-2022-22932	Apache Karaf obr:* commands and run goal on the karaf-maven-plugin have partial path traversal which allows to break out of expected folder. The risk is low as obr:* commands are not very used and the entry is set by user. This has been fixed in revision: https://gitbox.apache.org/repos/asf?p=karaf.git;h=36a2bc4 https://gitbox.apache.org/repos/asf?p=karaf.git;h=52b70cf Mitigation: Apache Karaf users should upgrade to 4.2.15 or 4.3.6 or later as soon as possible, or use correct path. JIRA Tickets: https://issues.apache.org/jira/browse/KARAF-7326	5.3	More Details
CVE-2022-23889	The comment function in YzmCMS v6.3 was discovered as being able to be operated concurrently, allowing attackers to create an unusually large number of comments.	5.3	More Details
CVE-2022-21659	Flask-AppBuilder is an application development framework, built on top of the Flask web framework. In affected versions there exists a user enumeration vulnerability. This vulnerability allows for a non authenticated user to enumerate existing accounts by timing the response time from the server when you are logging in. Users are advised to upgrade to version 3.4.4 as soon as possible. There are no known workarounds for this issue.	5.3	More Details
	A CWE-200: Information Exposure vulnerability exists which could cause the troubleshooting archive to be accessed. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA,		

CVE Number	Description	Base Score	Reference
	G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3		
CVE-2021-22815	including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)	5.3	More Details
CVE-2022-23774	Docker Desktop before 4.4.4 on Windows allows attackers to move arbitrary files.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24032	Adenza AxiomSL ControllerView through 10.8.1 is vulnerable to user enumeration. An attacker can identify valid usernames on the platform because a failed login attempt produces a different error message when the username is valid.	5.3	More Details
CVE-2022-23409	The Logs plugin before 3.0.4 for Craft CMS allows remote attackers to read arbitrary files via input to actionStream in Controller.php.	4.9	More Details
CVE-2022-21720	GLPI is a free asset and IT management software package. Prior to version 9.5.7, an entity administrator is capable of retrieving normally inaccessible data via SQL injection. Version 9.5.7 contains a patch for this issue. As a workaround, disabling the `Entities` update right prevents exploitation of this vulnerability.	4.9	More Details
CVE-2022-22868	Gibbon CMS v22.0.01 was discovered to contain a cross-site scripting (XSS) vulnerability, that allows attackers to inject arbitrary script via name parameters.	4.8	More Details
CVE-2022-0375	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	4.8	More Details
CVE-2021-44114	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Stock Management System in PHP/OOP 1.0, which allows remote malicious users to execute arbitrary remote code execution via create user function.	4.8	More Details
CVE-2022-23872	Emlog pro v1.1.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /admin/configure.php via the parameter footer_info.	4.8	More Details
CVE-2021-46065	A Cross-site scripting (XSS) vulnerability in Secondary Email Field in Zoho ManageEngine ServiceDesk Plus 11.3 Build 11306 allows an attackers to inject arbitrary JavaScript code.	4.8	More Details
CVE-2021-24707	The Learning Courses WordPress plugin before 5.0 does not sanitise and escape the Email PDT identity token settings, which could allow high privilege users to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-23979	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability discovered in Ultimate Reviews WordPress plugin (versions <= 3.0.15).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24900	The Ninja Tables WordPress plugin before 4.1.8 does not sanitise and escape some of its table fields, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24686	The SVG Support WordPress plugin before 2.3.20 does not escape the "CSS Class to target" setting before outputting it in an attribute, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24944	The Custom Dashboard & Login Page WordPress plugin before 7.0 does not sanitise some of its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-41166	The Nextcloud Android app is the Android client for Nextcloud, a self-hosted productivity platform. An issue in versions prior to 3.17.1 may lead to sensitive information disclosure. An unauthorized app that does not have the otherwise required `MANAGE_DOCUMENTS` permission may view image thumbnails for images it does not have permission to view. Version 3.17.1 contains a patch. There are no known workarounds.	4.3	More Details
CVE-2022-23599	Products.ATContentTypes are the core content types for Plone 2.1 - 4.3. Versions of Plone that are dependent on Products.ATContentTypes prior to version 3.0.6 are vulnerable to reflected cross site scripting and open redirect when an attacker can get a compromised version of the image_view_fullscreen page in a cache, for example in Varnish. The technique is known as cache poisoning. Any later visitor can get redirected when clicking on a link on this page. Usually only anonymous users are affected, but this depends on the user's cache settings. Version 3.0.6 of Products.ATContentTypes has been released with a fix. This version works on Plone 5.2, Python 2 only. As a workaround, make sure the image_view_fullscreen page is not stored in the cache. More information about the vulnerability and cvmitigation measures is available in the GitHub Security Advisory.	4.3	More Details
CVE-2022-24071	A Built-in extension in Whale browser before 3.12.129.46 allows attackers to compromise the rendering process which could lead to controlling browser internal APIs.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22819	A CWE-1021 Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the web interface rendered within iframes. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)	4.3	More Details
CVE-2021-24868	The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.	4.3	More Details
CVE-2022-0414	Improper Validation of Specified Quantity in Input in Packagist dolibarr/dolibarr prior to 16.0.	4.3	More Details
CVE-2021-32841	SharpZipLib (or #ziplib) is a Zip, GZip, Tar and BZip2 library. Starting version 1.3.0 and prior to version 1.3.3, a check was added if the destination file is under destination directory. However, it is not enforced that `destDir` ends with slash. If the `destDir` is not slash terminated like `/home/user/dir` it is possible to create a file with a name thats begins with the destination directory, i.e. `/home/user/dir.sh`. Because of the file name and destination directory constraints, the arbitrary file creation impact is limited and depends on the use case. Version 1.3.3 contains a patch for this vulnerability.	4.0	More Details
CVE-2021-32842	SharpZipLib (or #ziplib) is a Zip, GZip, Tar and BZip2 library. Starting version 1.0.0 and prior to version 1.3.3, a check was added if the destination file is under a destination directory. However, it is not enforced that `_baseDirectory` ends with slash. If the _baseDirectory is not slash terminated like `/home/user/dir` it is possible to create a file with a name thats begins as the destination directory one level up from the directory, i.e. `/home/user/dir.sh`. Because of the file name and destination directory constraints, the arbitrary file creation impact is limited and depends on the use case. Version 1.3.3 fixed this vulnerability.	4.0	More Details
CVE-2021-22799	A CWE-331: Insufficient Entropy vulnerability exists that could cause unintended connection from an internal network to an external network when an attacker manages to decrypt the SESU proxy password from the registry. Affected Product: Schneider Electric Software Update, V2.3.0 through V2.5.1	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40340	Information Exposure vulnerability in Hitachi Energy LinkOne application, due to a misconfiguration in the ASP server exposes server and ASP.net information, an attacker that manages to exploit this vulnerability can use the exposed information as a reconnaissance for further exploitation. This issue affects: Hitachi Energy LinkOne 3.20; 3.22; 3.23; 3.24; 3.25; 3.26.	3.7	More Details
CVE-2021-40339	Configuration vulnerability in Hitachi Energy LinkOne application due to the lack of HTTP Headers, allows an attacker that manages to exploit this vulnerability to retrieve sensitive information. This issue affects: Hitachi Energy LinkOne 3.20; 3.22; 3.23; 3.24; 3.25; 3.26.	3.7	More Details
CVE-2021-40338	Hitachi Energy LinkOne product, has a vulnerability due to a web server misconfiguration, that enables debug mode and reveals the full path of the filesystem directory when an attacker generates errors during a query operation. This issue affects: Hitachi Energy LinkOne 3.20; 3.22; 3.23; 3.24; 3.25; 3.26.	3.7	More Details
CVE-2021-23174	Authenticated (admin+) Persistent Cross-Site Scripting (XSS) vulnerability discovered in Download Monitor WordPress plugin (versions <= 4.4.6) Vulnerable parameters: &post_title, &downloadable_file_version[0].	3.4	More Details
CVE-2021-29846	IBM Security Guardium Insights 3.0 could allow an authenticated user to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 205256.	2.7	More Details
CVE-2020-8562	As mitigations to a report from 2019 and CVE-2020-8555, Kubernetes attempts to prevent proxied connections from accessing link-local or localhost networks when making user-driven connections to Services, Pods, Nodes, or StorageClass service providers. As part of this mitigation Kubernetes does a DNS name resolution check and validates that response IPs are not in the link-local (169.254.0.0/16) or localhost (127.0.0.0/8) range. Kubernetes then performs a second DNS resolution without validation for the actual connection. If a non-standard DNS server returns different non-cached responses, a user may be able to bypass the proxy IP restriction and access private networks on the control plane.	2.2	More Details
CVE-2022-23967	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-15679. Reason: This candidate is a duplicate of CVE-2019-15679. Notes: All CVE users should reference CVE-2019-15679 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-44121	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40395	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-3534	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-34981. Reason: This candidate is a reservation duplicate of CVE-2021-34981. Notes: All CVE users should reference CVE-2021-34981 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details