SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 October 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-42150	TinyLab linux-lab v1.1-rc1 and cloud-labv0.8-rc2, v1.1-rc1 are vulnerable to insecure permissions. The default configuration could cause Container Escape.	10.0	More Details
CVE-2023-35084	Unsafe Deserialization of User Input could lead to Execution of Unauthorized Operations in Ivanti Endpoint Manager 2022 su3 and all previous versions, which could allow an attacker to execute commands remotely.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38545	This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake. When curl is asked to pass along the host name to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that host name can be is 255 bytes. If the host name is detected to be longer, curl switches to local name resolving and instead passes on the resolved address only. Due to this bug, the local variable that means "let the host resolve the name" could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long host name to the target buffer instead of copying just the resolved address there. The target buffer being a heap based buffer, and the host name coming from the URL that curl has been told to operate with.	9.8	More Details
CVE-2023-45381	In the module "Creative Popup" (creativepopup) up to version 1.6.9 from WebshopWorks for PrestaShop, a guest can perform SQL injection via `cp_download_popup().`	9.8	More Details
CVE-2023-38584	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication.	9.8	More Details
CVE-2023-43492	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication.	9.8	More Details
CVE-2023-45376	In the module "Carousels Pack - Instagram, Products, Brands, Supplier" (hicarouselspack) for PrestaShop up to version 1.5.0 from HiPresta for PrestaShop, a guest can perform SQL injection via HiCpProductGetter::getViewedProduct().`	9.8	More Details
CVE-2023-30131	An issue discovered in IXP EasyInstall 6.6.14884.0 allows attackers to run arbitrary commands, gain escalated privilege, and cause other unspecified impacts via unauthenticated API calls.	9.8	More Details
CVE-2023-34051	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution.	9.8	More Details
CVE-2020-36706	The Simple:Press – WordPress Forum Plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ~/admin/resources/jscript/ajaxupload/sf-uploader.php file in versions up to, and including, 6.6.0. This makes it possible for attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4488	The Dropbox Folder Share for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 1.9.7 via the editor-view.php file. This allows unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	9.8	More Details
CVE-2023-37824	Sitolog sitologapplicationconnect v7.8.a and before was discovered to contain a SQL injection vulnerability via the component /activate_hook.php.	9.8	More Details
CVE-2023-46300	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of certain escape sequences related to tmux integration.	9.8	More Details
CVE-2023-46301	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of certain escape sequences related to upload.	9.8	More Details
CVE-2023-46321	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize paths in x-man-page URLs. They may have shell metacharacters for a /usr/bin/man command line.	9.8	More Details
CVE-2023-46322	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize ssh hostnames in URLs. The hostname's initial character may be non-alphanumeric. The hostname's other characters may be outside the set of alphanumeric characters, dash, and period.	9.8	More Details
CVE-2023-27152	DECISO OPNsense 23.1 does not impose rate limits for authentication, allowing attackers to perform a brute-force attack to bypass authentication.	9.8	More Details
CVE-2023-43986	DM Concept configurator before v4.9.4 was discovered to contain a SQL injection vulnerability via the component ConfiguratorAttachment::getAttachmentByToken.	9.8	More Details
CVE-2023-37635	UVDesk Community Skeleton v1.1.1 allows unauthenticated attackers to perform brute force attacks on the login page to gain access to the application.	9.8	More Details
CVE-2022-47583	Terminal character injection in Mintty before 3.6.3 allows code execution via unescaped output to the terminal.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46006	Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_user.php.	9.8	More Details
CVE-2023-45384	KnowBand supercheckout > 5.0.7 and < 6.0.7 is vulnerable to Unrestricted Upload of File with Dangerous Type. In the module "Module One Page Checkout, Social Login & Mailchimp" (supercheckout), a guest can upload files with extensions .php	9.8	More Details
CVE-2023-45379	In the module "Rotator Img" (posrotatorimg) in versions at least up to 1.1 from PosThemes for PrestaShop, a guest can perform SQL injection.	9.8	More Details
CVE-2023-5204	The ChatBot plugin for WordPress is vulnerable to SQL Injection via the $strid parameter in versions up to, and including, 4.8.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2023-46042	An issue in GetSimpleCMS v.3.4.0a allows a remote attacker to execute arbitrary code via a crafted payload to the phpinfo().	9.8	More Details
CVE-2023-39332	Various `node:fs` functions allow specifying paths as either strings or `Uint8Array` objects. In Node.js environments, the `Buffer` class extends the `Uint8Array` class. Node.js prevents path traversal through strings (see CVE-2023-30584) and `Buffer` objects (see CVE-2023-32004), but not through non-`Buffer` `Uint8Array` objects. This is distinct from CVE-2023-32004 which only referred to `Buffer` objects. However, the vulnerability follows the same pattern using `Uint8Array` instead of `Buffer`. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	9.8	More Details
CVE-2023-46005	Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_branch.php.	9.8	More Details
CVE-2023-45911	An issue in WIPOTEC GmbH ComScale v4.3.29.21344 and v4.4.12.723 allows unauthenticated attackers to login as any user without a password.	9.8	More Details
CVE-2023-5642	Advantech R-SeeNet v2.4.23 allows an unauthenticated remote attacker to read from and write to the snmpmon.ini file, which contains sensitive information.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46007	Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_staff.php.	9.8	More Details
CVE-2023-45992	A vulnerability in the web-based interface of the RUCKUS Cloudpath product on version 5.12 build 5538 or before to could allow a remote, unauthenticated attacker to execute persistent XSS and CSRF attacks against a user of the admin management interface. A successful attack, combined with a certain admin activity, could allow the attacker to gain full admin privileges on the exploited system.	9.6	More Details
CVE-2022-37830	Interway a.s WebJET CMS 8.6.896 is vulnerable to Cross Site Scripting (XSS).	9.6	More Details
CVE-2022-26941	A format string vulnerability exists in Motorola MTM5000 series firmware AT command handler for the AT+CTGL command. An attacker-controllable string is improperly handled, allowing for a write-anything-anywhere scenario. This can be leveraged to obtain arbitrary code execution inside the teds_app binary, which runs with root privileges.	9.6	More Details
CVE-2023-5241	The AI ChatBot for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.8.9 as well as 4.9.2 via the qcld_openai_upload_pagetraining_file function. This allows subscriber-level attackers to append "<?php" to any existing file on the server resulting in potential DoS when appended to critical files such as wp-config.php.	9.6	More Details
CVE-2023-5212	The AI ChatBot plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 4.8.9 as well as version 4.9.2. This makes it possible for authenticated attackers with subscriber privileges to delete arbitrary files on the server, which makes it possible to take over affected sites as well as others sharing the same hosting account. Version 4.9.1 originally addressed the issue, but it was reintroduced in 4.9.2 and fixed again in 4.9.3.	9.6	More Details
CVE-2023-45278	Directory Traversal vulnerability in the storage functionality of the API in Yamcs 5.8.6 allows attackers to delete arbitrary files via crafted HTTP DELETE request.	9.1	More Details
CVE-2023-5414	The Icegram Express plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 5.6.23 via the show_es_logs function. This allows administrator-level attackers to read the contents of arbitrary files on the server, which can contain sensitive information including those belonging to other sites, for example in shared hosting environments.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45146	XXL-RPC is a high performance, distributed RPC framework. With it, a TCP server can be set up using the Netty framework and the Hessian serialization mechanism. When such a configuration is used, attackers may be able to connect to the server and provide malicious serialized objects that, once deserialized, force it to execute arbitrary code. This can be abused to take control of the machine the server is running by way of remote code execution. This issue has not been fixed.	9.0	More Details
CVE-2023-37502	HCL Compass is vulnerable to lack of file upload security. An attacker could upload files containing active code that can be executed by the server or by a user's web browser.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-38193	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows Remote Code Execution via a crafted sendmail command line.	8.8	More Details
CVE-2023-23373	An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later	8.8	More Details
CVE-2023-38190	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows Export SQL Injection via the size parameter.	8.8	More Details
CVE-2023-46603	In International Color Consortium DemoIccMAX 79ecb74, there is an out-of-bounds read in the CIccPRMG::GetChroma function in IccProfLib/IccPrmg.cpp in libSampleICC.a.	8.8	More Details
CVE-2023-40145	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device.	8.8	More Details
CVE-2023-5246	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5687	Cross-Site Request Forgery (CSRF) in GitHub repository mosparo/mosparo prior to 1.0.3.	8.8	More Details
CVE-2023-46055	An issue in ThingNario Photon v.1.0 allows a remote attacker to execute arbitrary code and escalate privileges via a crafted script to the ping function to the "thingnario Logger Maintenance Webpage" endpoint.	8.8	More Details
CVE-2023-42295	An issue in OpenImageIO oiio v.2.4.12.0 allows a remote attacker to execute arbitrary code and cause a denial of service via the read_rle_image function of file bifs/unquantize.c	8.8	More Details
CVE-2023-5690	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.2.2.	8.8	More Details
CVE-2023-5336	The iPanorama 360 – WordPress Virtual Tour Builder plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 1.8.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-41895	Home assistant is an open source home automation. The Home Assistant login page allows users to use their local Home Assistant credentials and log in to another website that specifies the `redirect_uri` and `client_id` parameters. Although the `redirect_uri` validation typically ensures that it matches the `client_id` and the scheme represents either `http` or `https`, Home Assistant will fetch the `client_id` and check for `<link rel="redirect_uri" href="...">` HTML tags on the page. These URLs are not subjected to the same scheme validation and thus allow for arbitrary JavaScript execution on the Home Assistant administration page via usage of `javascript:` scheme URIs. This Cross-site Scripting (XSS) vulnerability can be executed on the Home Assistant frontend domain, which may be used for a full takeover of the Home Assistant account and installation. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-5626	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/ojs prior to 3.3.0-16.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46229	LangChain before 0.0.317 allows SSRF via document_loaders/recursive_url_loader.py because crawling can proceed from an external server to an internal server.	8.8	More Details
CVE-2020-36698	The Security & Malware scan by CleanTalk plugin for WordPress is vulnerable to unauthorized user interaction in versions up to, and including, 2.50. This is due to missing capability checks on several AJAX actions and nonce disclosure in the source page of the administrative dashboard. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to call functions and delete and/or upload files.	8.8	More Details
CVE-2023-41897	Home assistant is an open source home automation. Home Assistant server does not set any HTTP security headers, including the X-Frame-Options header, which specifies whether the web page is allowed to be framed. The omission of this and correlating headers facilitates covert clickjacking attacks and alternative exploit opportunities, such as the vector described in this security advisory. This fault incurs major risk, considering the ability to trick users into installing an external and malicious add-on with minimal user interaction, which would enable Remote Code Execution (RCE) within the Home Assistant application. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2021-4334	The Fancy Product Designer plugin for WordPress is vulnerable to unauthorized modification of site options due to a missing capability check on the fpd_update_options function in versions up to, and including, 4.6.9. This makes it possible for authenticated attackers with subscriber-level permissions to modify site options, including setting the default role to administrator which can allow privilege escalation.	8.8	More Details
CVE-2022-24401	Adversary-induced keystream re-use on TETRA air-interface encrypted traffic using any TEA keystream generator. IV generation is based upon several TDMA frame counters, which are frequently broadcast by the infrastructure in an unauthenticated manner. An active adversary can manipulate the view of these counters in a mobile station, provoking keystream re-use. By sending crafted messages to the MS and analyzing MS responses, keystream for arbitrary frames can be recovered.	8.8	More Details
CVE-2022-24402	The TETRA TEA1 keystream generator implements a key register initialization function that compresses the 80-bit key to only 32 bits for usage during the keystream generation phase, which is insufficient to safeguard against exhaustive search attacks.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4999	The Horizontal scrolling announcement plugin for WordPress is vulnerable to SQL Injection via the plugin's [horizontal-scrolling] shortcode in versions up to, and including, 9.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-46602	In International Color Consortium DemoIccMAX 79ecb74, there is a stack-based buffer overflow in the icFixXml function in IccXML/IccLibXML/IccUtilXml.cpp in libIccXML.a.	8.8	More Details
CVE-2022-26943	The Motorola MTM5000 series firmwares generate TETRA authentication challenges using a PRNG using a tick count register as its sole entropy source. Low boottime entropy and limited re-seeding of the pool renders the authentication challenge vulnerable to two attacks. First, due to the limited boottime pool entropy, an adversary can derive the contents of the entropy pool by an exhaustive search of possible values, based on an observed authentication challenge. Second, an adversary can use knowledge of the entropy pool to predict authentication challenges. As such, the unit is vulnerable to CVE-2022-24400.	8.8	More Details
CVE-2023-4598	The Slimstat Analytics plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 5.0.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2023-35182	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability can be abused by unauthenticated users on SolarWinds ARM Server.	8.8	More Details
CVE-2023-35184	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an unauthenticated user to abuse a SolarWinds service resulting in a remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46117	reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities. A vulnerability has been identified in reconftw where inadequate validation of retrieved subdomains may lead to a Remote Code Execution (RCE) attack. An attacker can exploit this vulnerability by crafting a malicious CSP entry on it's own domain. Successful exploitation can lead to the execution of arbitrary code within the context of the application, potentially compromising the system. This issue has been addressed in version 2.7.1.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-35187	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability. This vulnerability allows an unauthenticated user to achieve the Remote Code Execution.	8.8	More Details
CVE-2022-2441	The ImageMagick Engine plugin for WordPress is vulnerable to remote code execution via the 'cli_path' parameter in versions up to, and including 1.7.5. This makes it possible for unauthenticated users to run arbitrary commands leading to remote command execution, granted they can trick a site administrator into performing an action such as clicking on a link. This makes it possible for an attacker to create and or modify files hosted on the server which can easily grant attackers backdoor access to the affected server.	8.8	More Details
CVE-2022-4290	The Cyr to Lat plugin for WordPress is vulnerable to authenticated SQL Injection via the 'ctl_sanitize_title' function in versions up to, and including, 3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This potentially allows authenticated users with the ability to add or modify terms or tags to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. A partial patch became available in version 3.6 and the issue was fully patched in version 3.7.	8.8	More Details
CVE-2023-5686	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.9.0.	8.8	More Details
CVE-2023-4274	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 0.9.89. This allows authenticated attackers with administrative privileges to delete the contents of arbitrary directories on the server, which can be a critical issue in a shared environments.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5523	Execution of downloaded content flaw in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution	8.6	More Details
CVE-2023-44385	The Home Assistant Companion for iOS and macOS app up to version 2023.4 are vulnerable to Client-Side Request Forgery. Attackers may send malicious links/QRs to victims that, when visited, will make the victim to call arbitrary services in their Home Assistant installation. Combined with this security advisory, may result in full compromise and remote code execution (RCE). Version 2023.7 addresses this issue and all users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GitHub Security Lab (GHSL) Vulnerability Report: GHSL-2023-161.	8.6	More Details
CVE-2023-43345	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the Content - Name parameter in the Pages Menu component.	8.6	More Details
CVE-2023-41898	Home assistant is an open source home automation. The Home Assistant Companion for Android app up to version 2023.8.2 is vulnerable to arbitrary URL loading in a WebView. This enables all sorts of attacks, including arbitrary JavaScript execution, limited native code execution, and credential theft. This issue has been patched in version 2023.9.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2023-142`.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46115	Tauri is a framework for building binaries for all major desktop platforms. This advisory is not describing a vulnerability in the Tauri code base itself but a commonly used misconfiguration which could lead to leaking of the private key and updater key password into bundled Tauri applications using the Vite frontend in a specific configuration. The Tauri documentation used an insecure example configuration in the `Vite guide` to showcase how to use Tauri together with Vite. Copying the following snippet `envPrefix: ['VITE_', 'TAURI_'],` from this guide into the `vite.config.ts` of a Tauri project leads to bundling the `TAURI_PRIVATE_KEY` and `TAURI_KEY_PASSWORD` into the Vite frontend code and therefore leaking this value to the released Tauri application. Using the `envPrefix: ['VITE_'],` or any other framework than Vite means you are not impacted by this advisory. Users are advised to rotate their updater private key if they are affected by this (requires Tauri CLI >=1.5.5). After updating the envPrefix configuration, generate a new private key with `tauri signer generate`, saving the new private key and updating the updater's `pubkey` value on `tauri.conf.json` with the new public key. To update your existing application, the next application build must be signed with the older private key in order to be accepted by the existing application.	8.4	More Details
CVE-2023-46306	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105.	8.4	More Details
CVE-2022-25334	The Texas Instruments OMAP L138 (secure variants) trusted execution environment (TEE) lacks a bounds check on the signature size field in the SK_LOAD module loading routine, present in mask ROM. A module with a sufficiently large signature field causes a stack overflow, affecting secure kernel data pages. This can be leveraged to obtain arbitrary code execution in secure supervisor context by overwriting a SHA256 function pointer in the secure kernel data area when loading a forged, unsigned SK_LOAD module encrypted with the CEK (obtainable through CVE-2022-25332). This constitutes a full break of the TEE security architecture.	8.2	More Details
CVE-2023-5524	Insufficient blacklisting in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution via specific file types	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28804	An Improper Verification of Cryptographic Signature vulnerability in Zscaler Client Connector on Linux allows replacing binaries.This issue affects Linux Client Connector: before 1.4.0.105	8.2	More Details
CVE-2022-25333	The Texas Instruments OMAP L138 (secure variants) trusted execution environment (TEE) performs an RSA check implemented in mask ROM when loading a module through the SK_LOAD routine. However, only the module header authenticity is validated. An adversary can re-use any correctly signed header and append a forged payload, to be encrypted using the CEK (obtainable through CVE-2022-25332) in order to obtain arbitrary code execution in secure context. This constitutes a full break of the TEE security architecture.	8.2	More Details
CVE-2022-26942	The Motorola MTM5000 series firmwares lack pointer validation on arguments passed to trusted execution environment (TEE) modules. Two modules are used, one responsible for KVL key management and the other for TETRA cryptographic functionality. In both modules, an adversary with non-secure supervisor level code execution can exploit the issue in order to gain secure supervisor code execution within the TEE. This constitutes a full break of the TEE module, exposing the device key as well as any TETRA cryptographic keys and the confidential TETRA cryptographic primitives.	8.2	More Details
CVE-2023-37503	HCL Compass is vulnerable to insecure password requirements. An attacker could easily guess the password and gain access to user accounts.	8.1	More Details
CVE-2023-4601	A stack-based buffer overflow vulnerability exists in NI System Configuration that could result in information disclosure and/or arbitrary code execution. Successful exploitation requires that an attacker can provide a specially crafted response. This affects NI System Configuration 2023 Q3 and all previous versions.	8.1	More Details
CVE-2023-4386	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_posts function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.1	More Details
CVE-2023-27791	An issue found in IXP Data Easy Install 6.6.148840 allows a remote attacker to escalate privileges via insecure PRNG.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27813	Motorola MTM5000 series firmwares lack properly configured memory protection of pages shared between the OMAP-L138 ARM and DSP cores. The SoC provides two memory protection units, MPU1 and MPU2, to enforce the trust boundary between the two cores. Since both units are left unconfigured by the firmwares, an adversary with control over either core can trivially gain code execution on the other, by overwriting code located in shared RAM or DDR2 memory regions.	8.1	More Details
CVE-2023-4402	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_products function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.1	More Details
CVE-2023-35180	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API.	8.0	More Details
CVE-2023-41089	The affected product is vulnerable to an improper authentication vulnerability, which may allow an attacker to impersonate a legitimate user as long as the device keeps the session active, since the attack takes advantage of the cookie header to generate "legitimate" requests.	8.0	More Details
CVE-2023-35186	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution.	8.0	More Details
CVE-2023-5576	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 0.9.91 via Google Drive API secrets stored in plaintext in the publicly visible plugin source. This could allow unauthenticated attackers to impersonate the WPVivid Google Drive account via the API if they can trick a user into reauthenticating via another vulnerability or social engineering.	8.0	More Details
CVE-2023-5633	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware guest with 3D acceleration enabled, a local, unprivileged user could potentially use this flaw to escalate their privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40361	SECUDOS Qiata (DOMOS OS) 4.13 has Insecure Permissions for the previewRm.sh daily cronjob. To exploit this, an attacker needs access as a low-privileged user to the underlying DOMOS system. Every user on the system has write permission for previewRm.sh, which is executed by the root user.	7.8	More Details
CVE-2023-46228	zchunk before 1.3.2 has multiple integer overflows via malformed zchunk files to lib/comp/comp.c, lib/comp/zstd/zstd.c, lib/dl/multipart.c, or lib/header.c.	7.8	More Details
CVE-2021-26738	Zscaler Client Connector for macOS prior to 3.7 had an unquoted search path vulnerability via the PATH variable. A local adversary may be able to execute code with root privileges.	7.8	More Details
CVE-2023-35181	The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation.	7.8	More Details
CVE-2023-43252	XNSoft Nconvert 7.136 is vulnerable to Buffer Overflow via a crafted image file.	7.8	More Details
CVE-2023-45883	A privilege escalation vulnerability exists within the Qumu Multicast Extension v2 before 2.0.63 for Windows. When a standard user triggers a repair of the software, a pop-up window opens with SYSTEM privileges. Standard users may use this to gain arbitrary code execution as SYSTEM.	7.8	More Details
CVE-2023-35183	The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation.	7.8	More Details
CVE-2023-43251	XNSoft Nconvert 7.136 has an Exception Handler Chain Corrupted via a crafted image file. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution.	7.8	More Details
CVE-2023-35126	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34366	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-35986	Sante DICOM Viewer Pro lacks proper validation of user-supplied data when parsing DICOM files. This could lead to a stack-based buffer overflow. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-38127	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-38128	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-39431	Sante DICOM Viewer Pro lacks proper validation of user-supplied data when parsing DICOM files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-5059	Santesoft Sante FFT Imaging lacks proper validation of user-supplied data when parsing DICOM files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-28793	Buffer overflow vulnerability in the signelf library used by Zscaler Client Connector on Linux allows Code Injection. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	7.8	More Details
CVE-2023-27792	An issue found in IXP Data Easy Install v.6.6.14884.0 allows an attacker to escalate privileges via lack of permissions applied to sub directories.	7.8	More Details
CVE-2023-30132	An issue discovered in IXP Data EasyInstall 6.6.14907.0 allows attackers to gain escalated privileges via static Cryptographic Key.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45805	pdm is a Python package and dependency manager supporting the latest PEP standards. It's possible to craft a malicious `pdm.lock` file that could allow e.g. an insider or a malicious open source project to appear to depend on a trusted PyPI project, but actually install another project. A project `foo` can be targeted by creating the project `foo-2` and uploading the file `foo-2-2.tar.gz` to pypi.org. PyPI will see this as project `foo-2` version `2`, while PDM will see this as project `foo` version `2-2`. The version must only be `parseable as a version` and the filename must be a prefix of the project name, but it's not verified to match the version being installed. Version `2-2` is also not a valid normalized version per PEP 440. Matching the project name exactly (not just prefix) would fix the issue. When installing dependencies with PDM, what's actually installed could differ from what's listed in `pyproject.toml` (including arbitrary code execution on install). It could also be used for downgrade attacks by only changing the version. This issue has been addressed in commit `6853e2642df` which is included in release version `2.9.4`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.8	More Details
CVE-2023-27795	An issue found in IXP Data Easy Install v.6.6.14884.0 allows a local attacker to gain privileges via a static XOR key.	7.8	More Details
CVE-2023-46277	please (aka pleaser) through 0.5.4 allows privilege escalation through the TIOCSTI and/or TIOCLINUX ioctl. (If both TIOCSTI and TIOCLINUX are disabled, this cannot be exploited.)	7.8	More Details
CVE-2023-43250	XNSoft Nconvert 7.136 is vulnerable to Buffer Overflow. There is a User Mode Write AV via a crafted image file. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution.	7.8	More Details
CVE-2023-34052	VMware Aria Operations for Logs contains a deserialization vulnerability. A malicious actor with non-administrative access to the local system can trigger the deserialization of data which could result in authentication bypass.	7.8	More Details
CVE-2023-27793	An issue discovered in IXP Data Easy Install v.6.6.14884.0 allows local attackers to gain escalated privileges via weak encoding of sensitive information.	7.8	More Details
CVE-2023-46009	gifsicle-1.94 was found to have a floating point exception (FPE) vulnerability via resize_stream at src/xform.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26300	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	7.8	More Details
CVE-2023-28795	Origin Validation Error vulnerability in Zscaler Client Connector on Linux allows Inclusion of Code in Existing Process. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	7.8	More Details
CVE-2023-3487	An integer overflow in Silicon Labs Gecko Bootloader version 4.3.1 and earlier allows unbounded memory access when reading from or writing to storage slots.	7.7	More Details
CVE-2023-39331	A previously disclosed vulnerability (CVE-2023-30584) was patched insufficiently in commit 205f1e6. The new path traversal vulnerability arises because the implementation does not protect itself against the application overwriting built-in utility functions with user-defined implementations. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	7.5	More Details
CVE-2023-45912	WIPOTEC GmbH ComScale v4.3.29.21344 and v4.4.12.723 fails to validate user sessions, allowing unauthenticated attackers to read files from the underlying operating system and obtain directory listings.	7.5	More Details
CVE-2023-38552	When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can intercept the operation and return a forged checksum to the node's policy implementation, thus effectively disabling the integrity check. Impacts: This vulnerability affects all users using the experimental policy mechanism in all active release lines: 18.x and, 20.x. Please note that at the time this CVE was issued, the policy mechanism is an experimental feature of Node.js.	7.5	More Details
CVE-2023-39680	Sollace Unicopia version 1.1.1 and before was discovered to deserialize untrusted data, allowing attackers to execute arbitrary code.	7.5	More Details
CVE-2023-44690	Inadequate encryption strength in mycli 1.27.0 allows attackers to view sensitive information via /mycli/config.py	7.5	More Details
CVE-2023-45277	Yamcs 5.8.6 is vulnerable to directory traversal (issue 1 of 2). The vulnerability is in the storage functionality of the API and allows one to escape the base directory of the buckets, freely navigate system directories, and read arbitrary files.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3342	The Jetpack CRM plugin for WordPress is vulnerable to PHAR deserialization via the ‘zbscrmcsvimpf’ parameter in the 'zeroBSCRM_CSVImporterLitehtml_app' function in versions up to, and including, 5.3.1. While the function performs a nonce check, steps 2 and 3 of the check do not take any action upon a failed check. These steps then perform a 'file_exists' check on the value of 'zbscrmcsvimpf'. If a phar:// archive is supplied, its contents will be deserialized and an object injected in the execution stream. This allows an unauthenticated attacker to obtain object injection if they are able to upload a phar archive (for instance if the site supports image uploads) and then trick an administrator into performing an action, such as clicking a link.	7.5	More Details
CVE-2023-32786	In Langchain through 0.0.155, prompt injection allows an attacker to force the service to retrieve data from an arbitrary URL, essentially providing SSRF and potentially injecting content into downstream tasks.	7.5	More Details
CVE-2023-45383	In the module "SoNice etiquetage" (sonice_etiquetage) up to version 2.5.9 from Common-Services for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack. Due to a lack of permissions control and a lack of control in the path name construction, a guest can perform a path traversal to view all files on the information system.	7.5	More Details
CVE-2023-45823	Artifact Hub is a web-based application that enables finding, installing, and publishing packages and configurations for CNCF projects. During a security audit of Artifact Hub's code base a security researcher identified a bug in which by using symbolic links in certain kinds of repositories loaded into Artifact Hub, it was possible to read internal files. Artifact Hub indexes content from a variety of sources, including git repositories. When processing git based repositories, Artifact Hub clones the repository and, depending on the artifact kind, reads some files from it. During this process, in some cases, no validation was done to check if the file was a symbolic link. This made possible to read arbitrary files in the system, potentially leaking sensitive information. This issue has been resolved in version `1.16.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-5132	The Soisy Pagamento Rateale plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the parseRemoteRequest function in versions up to, and including, 6.0.1. This makes it possible for unauthenticated attackers with knowledge of an existing WooCommerce Order ID to expose sensitive WooCommerce order information (e.g., Name, Address, Email Address, and other order metadata).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46317	Knot Resolver before 5.7.0 performs many TCP reconnections upon receiving certain nonsensical responses from servers.	7.5	More Details
CVE-2023-33517	carRental 1.0 is vulnerable to Incorrect Access Control (Arbitrary File Read on the Back-end System).	7.5	More Details
CVE-2023-46319	WALLIX Bastion 9.x before 9.0.9 and 10.x before 10.0.5 allows unauthenticated access to sensitive information by bypassing access control on a network access administration web interface.	7.5	More Details
CVE-2023-35656	In multiple functions of protocolembmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-42319	Geth (aka go-ethereum) through 1.13.4, when --http --graphql is used, allows remote attackers to cause a denial of service (memory consumption and daemon hang) via a crafted GraphQL query. NOTE: the vendor's position is that the "graphql endpoint [is not] designed to withstand attacks by hostile clients, nor handle huge amounts of clients/traffic.	7.5	More Details
CVE-2023-5632	In Eclipse Mosquito before and including 2.0.5, establishing a connection to the mosquitto server without sending data causes the EPOLLOUT event to be added, which results excessive CPU consumption. This could be used by a malicious actor to perform denial of service type attack. This issue is fixed in 2.0.6	7.5	More Details
CVE-2023-46315	The zanllp sd-webui-infinite-image-browsing (aka Infinite Image Browsing) extension before 977815a for stable-diffusion-webui (aka Stable Diffusion web UI), if Gradio authentication is enabled without secret key configuration, allows remote attackers to read any local file via /file?path= in the URL, as demonstrated by reading /proc/self/environ to discover credentials.	7.5	More Details
CVE-2023-45727	Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, and Proself Mail Sanitize Edition Ver1.08 and earlier allow a remote unauthenticated attacker to conduct XML External Entity (XXE) attacks. By processing a specially crafted request containing malformed XML data, arbitrary files on the server containing account information may be read by the attacker.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43622	An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.	7.5	More Details
CVE-2023-31122	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.	7.5	More Details
CVE-2022-24400	A flaw in the TETRA authentication procecure allows a MITM adversary that can predict the MS challenge RAND2 to set session key DCK to zero.	7.5	More Details
CVE-2023-46298	Next.js before 13.4.20-canary.13 lacks a cache-control header and thus empty prefetch responses may sometimes be cached by a CDN, causing a denial of service to all users requesting the same URL via that CDN.	7.5	More Details
CVE-2023-35663	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2022-4943	The miniOrange's Google Authenticator plugin for WordPress is vulnerable to authorization bypass due to a missing capability check when changing plugin settings in versions up to, and including, 5.6.5. This makes it possible for unauthenticated attackers to change the plugin's settings.	7.5	More Details
CVE-2023-46303	link_to_local_path in ebooks/conversion/plugins/html_input.py in calibre before 6.19.0 can, by default, add resources outside of the document root.	7.5	More Details
CVE-2023-34437	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a vulnerability in their password retrieval functionality which could allow an attacker to access passwords stored on the device.	7.5	More Details
CVE-2023-45966	umputun remark42 version 1.12.1 and before has a Blind Server-Side Request Forgery (SSRF) vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45812	The Apollo Router is a configurable, high-performance graph router written in Rust to run a federated supergraph that uses Apollo Federation. Affected versions are subject to a Denial-of-Service (DoS) type vulnerability which causes the Router to panic and terminate when a multi-part response is sent. When users send queries to the router that uses the `@defer` or Subscriptions, the Router will panic. To be vulnerable, users of Router must have a coprocessor with `coprocessor.supergraph.response` configured in their `router.yaml` and also to support either `@defer` or Subscriptions. Apollo Router version 1.33.0 has a fix for this vulnerability which was introduced in PR #4014. Users are advised to upgrade. Users unable to upgrade should avoid using the coprocessor supergraph response or disable defer and subscriptions support and continue to use the coprocessor supergraph response.	7.5	More Details
CVE-2023-46324	pkg/suci/suci.go in free5GC udm before 1.2.0, when Go before 1.19 is used, allows an Invalid Curve Attack because it may compute a shared secret via an uncompressed public key that has not been validated. An attacker can send arbitrary SUCIs to the UDM, which tries to decrypt them via both its private key and the attacker's public key.	7.5	More Details
CVE-2023-46227	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong. This issue affects Apache InLong: from 1.4.0 through 1.8.0, the attacker can use \t to bypass. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8814	7.5	More Details
CVE-2020-36714	The Brizy plugin for WordPress is vulnerable to authorization bypass due to a incorrect capability check on the is_administrator() function in versions up to, and including, 1.0.125. This makes it possible for authenticated attackers to access and interact with available AJAX functions.	7.4	More Details
CVE-2023-2325	Stored XSS Vulnerability in M-Files Classic Web versions before 23.10 and LTS Service Release Versions before 23.2 LTS SR4 and 23.8 LTS SR1allows attacker to execute script on users browser via stored HTML document.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45664	stb_image is a single file MIT licensed library for processing images. A crafted image file can trigger `stbi__load_gif_main_outofmem` attempt to double-free the out variable. This happens in `stbi__load_gif_main` because when the `layers * stride` value is zero the behavior is implementation defined, but common that realloc frees the old memory and returns null pointer. Since it attempts to double-free the memory a few lines below the first “free”, the issue can be potentially exploited only in a multi-threaded environment. In the worst case this may lead to code execution.	7.3	More Details
CVE-2023-45681	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory write past an allocated heap buffer in `start_decoder`. The root cause is a potential integer overflow in `sizeof(char*) * (f->comment_list_length)` which may make `setup_malloc` allocate less memory than required. Since there is another integer overflow an attacker may overflow it too to force `setup_malloc` to return 0 and make the exploit more reliable. This issue may lead to code execution.	7.3	More Details
CVE-2023-45677	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[len] = (char)'\0';`. The root cause is that if `len` read in `start_decoder` is a negative number and `setup_malloc` successfully allocates memory in that case, but memory write is done with a negative index `len`. Similarly if len is INT_MAX the integer overflow len+1 happens in `f->vendor = (char*)setup_malloc(f, sizeof(char) * (len+1));` and `f->comment_list[i] = (char*)setup_malloc(f, sizeof(char) * (len+1));`. This issue may lead to code execution.	7.3	More Details
CVE-2023-45666	stb_image is a single file MIT licensed library for processing images. It may look like `stbi__load_gif_main` doesn’t give guarantees about the content of output value `*delays` upon failure. Although it sets `*delays` to zero at the beginning, it doesn’t do it in case the image is not recognized as GIF and a call to `stbi__load_gif_main_outofmem` only frees possibly allocated memory in `*delays` without resetting it to zero. Thus it would be fair to say the caller of `stbi__load_gif_main` is responsible to free the allocated memory in `*delays` only if `stbi__load_gif_main` returns a non null value. However at the same time the function may return null value, but fail to free the memory in `*delays` if internally `stbi__convert_format` is called and fails. Thus the issue may lead to a memory leak if the caller chooses to free `delays` only when `stbi__load_gif_main` didn’t fail or to a double-free if the `delays` is always freed	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43800	Arduino Create Agent is a package to help manage Arduino development. The vulnerability affects the endpoint `/v2/pkgs/tools/installed`. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can escalate his privileges to those of the user running the Arduino Create Agent service via a crafted HTTP POST request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this issue.	7.3	More Details
CVE-2023-45679	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory allocation failure in `start_decoder`. In that case the function returns early, but some of the pointers in `f->comment_list` are left initialized and later `setup_free` is called on these pointers in `vorbis_deinit`. This issue may lead to code execution.	7.3	More Details
CVE-2023-45676	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[i] = get8_packet(f);`. The root cause is an integer overflow in `setup_malloc`. A sufficiently large value in the variable `sz` overflows with `sz+7` in and the negative value passes the maximum available memory buffer check. This issue may lead to code execution.	7.3	More Details
CVE-2022-4712	The WP Cerber Security plugin for WordPress is vulnerable to stored cross-site scripting via the log parameter when logging in to the site in versions up to, and including, 9.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-46004	Sourcecodester Best Courier Management System 1.0 is vulnerable to Arbitrary file upload in the update_user function.	7.2	More Details
CVE-2023-5538	The MpOperationLogs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the IP Request Headers in versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-33839	IBM Security Verify Governance 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 256036.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34044	VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine.	7.1	More Details
CVE-2023-45070	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in 10Web Form Builder Team Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin <= 1.15.18 versions.	7.1	More Details
CVE-2023-25476	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ezoic AmpedSense – AdSense Split Tester plugin <= 4.68 versions.	7.1	More Details
CVE-2023-45054	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in AWESOME TOGI Product Category Tree plugin <= 2.5 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41896	Home assistant is an open source home automation. Whilst auditing the frontend code to identify hidden parameters, Cure53 detected `auth_callback=1`, which is leveraged by the WebSocket authentication logic in tandem with the `state` parameter. The state parameter contains the `hassUrl`, which is subsequently utilized to establish a WebSocket connection. This behavior permits an attacker to create a malicious Home Assistant link with a modified state parameter that forces the frontend to connect to an alternative WebSocket backend. Henceforth, the attacker can spoof any WebSocket responses and trigger cross site scripting (XSS). Since the XSS is executed on the actual Home Assistant frontend domain, it can connect to the real Home Assistant backend, which essentially represents a comprehensive takeover scenario. Permitting the site to be iframed by other origins, as discussed in GHSA-935v-rmg9-44mw, renders this exploit substantially covert since a malicious website can obfuscate the compromise strategy in the background. However, even without this, the attacker can still send the `auth_callback` link directly to the victim user. To mitigate this issue, Cure53 advises modifying the WebSocket code's authentication flow. An optimal implementation in this regard would not trust the `hassUrl` passed in by a GET parameter. Cure53 must stipulate the significant time required of the Cure53 consultants to identify an XSS vector, despite holding full control over the WebSocket responses. In many areas, data from the WebSocket was properly sanitized, which hinders post-exploitation. The audit team eventually detected the `js_url` for custom panels, though generally, the frontend exhibited reasonable security hardening. This issue has been addressed in Home Assistant Core version 2023.8.0 and in the npm package home-assistant-js-websocket in version 8.2.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2023-45062	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Thomas Scholl canvasio3D Light plugin <= 2.4.6 versions.	7.1	More Details
CVE-2023-45064	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Daisuke Takahashi(Extend Wings) OPcache Dashboard plugin <= 0.3.1 versions.	7.1	More Details
CVE-2023-28796	Improper Verification of Cryptographic Signature vulnerability in Zscaler Client Connector on Linux allows Code Injection. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	7.1	More Details
CVE-2023-45065	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Mad Fish Digital Bulk NoIndex & NoFollow Toolkit plugin <= 1.42 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45602	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Shopfiles Ltd Ebook Store plugin <= 5.785 versions.	7.1	More Details
CVE-2023-5552	A password disclosure vulnerability in the Secure PDF eXchange (SPX) feature allows attackers with full email access to decrypt PDFs in Sophos Firewall version 19.5 MR3 (19.5.3) and older, if the password type is set to “Specified by sender”.	7.1	More Details
CVE-2023-45071	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in 10Web Form Builder Team Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin <= 1.15.18 versions.	7.1	More Details
CVE-2023-30781	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Theme Blvd Tweeple plugin <= 0.9.5 versions.	7.1	More Details
CVE-2023-45630	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in wpdevart Gallery – Image and Video Gallery with Thumbnails plugin <= 2.0.3 versions.	7.1	More Details
CVE-2023-45632	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WebDorado SpiderVPlayer plugin <= 1.5.22 versions.	7.1	More Details
CVE-2023-43802	Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint `/upload` which handles request with the `filename` parameter. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can escalate their privileges to those of the user running the Arduino Create Agent service via a crafted HTTP POST request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2023-37504	HCL Compass is vulnerable to failure to invalidate sessions. The application does not invalidate authenticated sessions when the log out functionality is called. If the session identifier can be discovered, it could be replayed to the application and used to impersonate the user.	7.1	More Details
CVE-2022-22466	IBM Security Verify Governance 10.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 225222.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35185	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability using SYSTEM privileges.	6.8	More Details
CVE-2023-30911	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service.	6.8	More Details
CVE-2023-34441	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a cleartext transmission vulnerability which could allow an attacker to steal the authentication secret from communication traffic to the device and reuse it for arbitrary requests.	6.8	More Details
CVE-2023-46033	D-Link (Non-US) DSL-2750U N300 ADSL2+ and (Non-US) DSL-2730U N150 ADSL2+ are vulnerable to Incorrect Access Control. The UART/Serial interface on the PCB, provides log output and a root terminal without proper access control.	6.8	More Details
CVE-2021-26735	The Zscaler Client Connector Installer and Unsintallers for Windows prior to 3.6 had an unquoted search path vulnerability. A local adversary may be able to execute code with SYSTEM privileges.	6.7	More Details
CVE-2023-28805	An Improper Input Validation vulnerability in Zscaler Client Connector on Linux allows Privilege Escalation. This issue affects Client Connector: before 1.4.0.105	6.7	More Details
CVE-2021-26736	Multiple vulnerabilities in the Zscaler Client Connector Installer and Uninstaller for Windows prior to 3.6 allowed execution of binaries from a low privileged path. A local adversary may be able to execute code with SYSTEM privileges.	6.7	More Details
CVE-2023-34046	VMware Fusion(13.x prior to 13.5) contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time.	6.7	More Details
CVE-2023-34045	VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41899	Home assistant is an open source home automation. In affected versions the `hassio.addon_stdin` is vulnerable to a partial Server-Side Request Forgery where an attacker capable of calling this service (e.g.: through GHSA-h2jp-7grc-9xpp) may be able to invoke any Supervisor REST API endpoints with a POST request. An attacker able to exploit will be able to control the data dictionary, including its addon and input key/values. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2023-162`.	6.6	More Details
CVE-2023-45628	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in QROkes QR Twitter Widget plugin <= 0.2.3 versions.	6.5	More Details
CVE-2023-31046	A Path Traversal vulnerability exists in PaperCut NG before 22.1.1 and PaperCut MF before 22.1.1. Under specific conditions, this could potentially allow an authenticated attacker to achieve read-only access to the server's filesystem, because requests beginning with "GET /ui/static/..//.." reach getStaticContent in UIContentResource.class in the static-content-files servlet.	6.5	More Details
CVE-2023-45662	stb_image is a single file MIT licensed library for processing images. When `stbi_set_flip_vertically_on_load` is set to `TRUE` and `req_comp` is set to a number that doesn’t match the real number of components per pixel, the library attempts to flip the image vertically. A crafted image file can trigger `memcpy` out-of-bounds read because `bytes_per_pixel` used to calculate `bytes_per_row` doesn’t match the real image array dimensions.	6.5	More Details
CVE-2023-5654	The React Developer Tools extension registers a message listener with window.addEventListener('message', <listener>) in a content script that is accessible to any webpage that is active in the browser. Within the listener is code that requests a URL derived from the received message via fetch(). The URL is not validated or sanitised before it is fetched, thus allowing a malicious web page to arbitrarily fetch URL’s via the victim's browser.	6.5	More Details
CVE-2023-5070	The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.8.5 via the sfsi_save_export function. This can allow subscribers to export plugin settings that include social media authentication tokens and secrets as well as app passwords.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45826	Leantime is an open source project management system. A 'userId' variable in `app/domain/files/repositories/class.files.php` is not parameterized. An authenticated attacker can send a carefully crafted POST request to `/api/jsonrpc` to exploit an SQL injection vulnerability. Confidentiality is impacted as it allows for dumping information from the database. This issue has been addressed in version 2.4-beta-4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-45675	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[len] = (char)'\0';`. The root cause is that if the len read in `start_decoder` is `-1` and `len + 1` becomes 0 when passed to `setup_malloc`. The `setup_malloc` behaves differently when `f->alloc.alloc_buffer` is pre-allocated. Instead of returning `NULL` as in `malloc` case it shifts the pre-allocated buffer by zero and returns the currently available memory block. This issue may lead to code execution.	6.5	More Details
CVE-2023-45678	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of buffer write in `start_decoder` because at maximum `m->submaps` can be 16 but `submap_floor` and `submap_residue` are declared as arrays of 15 elements. This issue may lead to code execution.	6.5	More Details
CVE-2023-20261	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	6.5	More Details
CVE-2023-25753	There exists an SSRF (Server-Side Request Forgery) vulnerability located at the /sandbox/proxyGateway endpoint. This vulnerability allows us to manipulate arbitrary requests and retrieve corresponding responses by inputting any URL into the requestUrl parameter. Of particular concern is our ability to exert control over the HTTP method, cookies, IP address, and headers. This effectively grants us the capability to dispatch complete HTTP requests to hosts of our choosing. This issue affects Apache ShenYu: 2.5.1. Upgrade to Apache ShenYu 2.6.0 or apply patch https://github.com/apache/shenyu/pull/4776 .	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45661	stb_image is a single file MIT licensed library for processing images. A crafted image file may trigger out of bounds memcpy read in `stbi__gif_load_next`. This happens because two_back points to a memory address lower than the start of the buffer out. This issue may be used to leak internal memory allocation information.	6.5	More Details
CVE-2023-45607	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Hector Cabrera WordPress Popular Posts plugin <= 6.3.2 versions.	6.5	More Details
CVE-2023-44256	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request.	6.5	More Details
CVE-2023-35083	Allows an authenticated attacker with network access to read arbitrary files on Endpoint Manager recently discovered on 2022 SU3 and all previous versions potentially leading to the leakage of sensitive information.	6.5	More Details
CVE-2021-46897	views.py in Wagtail CRX CodeRed Extensions (formerly CodeRed CMS or coderedcms) before 0.22.3 allows upward protected/..%2f..%2f path traversal when serving protected media.	6.5	More Details
CVE-2023-45067	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ashish Ajani WordPress Simple HTML Sitemap plugin <= 2.1 versions.	6.5	More Details
CVE-2023-31217	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in MyTechTalky User Location and IP plugin <= 1.6 versions.	6.5	More Details
CVE-2023-45059	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gumroad plugin <= 3.1.0 versions.	6.5	More Details
CVE-2023-45608	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Nicola Modugno Smart Cookie Kit plugin <= 2.3.1 versions.	6.5	More Details
CVE-2023-45049	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ciprian Popescu YouTube Playlist Player plugin <= 4.6.7 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44483	All versions of Apache Santuario - XML Security for Java prior to 2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is enabled. Users are recommended to upgrade to version 2.2.6, 2.3.4, or 3.0.3, which fixes this issue.	6.5	More Details
CVE-2023-5639	The Team Showcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tmfshortcode' shortcode in all versions up to, and including, 2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5205	The Add Custom Body Class plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'add_custom_body_class' value in versions up to, and including, 1.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5638	The Booster for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wcj_image' shortcode in versions up to, and including, 7.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5050	The Leaflet Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5071	The Sitekit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sitekit_iframe' shortcode in versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5200	The flowpaper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'flipbook' shortcode in versions up to, and including, 2.0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5308	The Podcast Subscribe Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'podcast_subscribe' shortcode in versions up to, and including, 1.4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4919	The iframe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `iframe` shortcode in versions up to, and including, 4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permission and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 4.6 and fully patched in version 4.7.	6.4	More Details
CVE-2023-4961	The Poptin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'poptin-form' shortcode in versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5668	The WhatsApp Share Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'whatsapp' shortcode in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45815	ArchiveBox is an open source self-hosted web archiving system. Any users who are using the `wget` extractor and view the content it outputs. The impact is potentially severe if you are logged in to the ArchiveBox admin site in the same browser session and view an archived malicious page designed to target your ArchiveBox instance. Malicious Javascript could potentially act using your logged-in admin credentials and add/remove/modify snapshots, add/remove/modify ArchiveBox users, and generally do anything an admin user could do. The impact is less severe for non-logged-in users, as malicious Javascript cannot *modify* any archives, but it can still *read* all the other archived content by fetching the snapshot index and iterating through it. Because all of ArchiveBox's archived content is served from the same host and port as the admin panel, when archived pages are viewed the JS executes in the same context as all the other archived pages (and the admin panel), defeating most of the browser's usual CORS/CSRF security protections and leading to this issue. A patch is being developed in https://github.com/ArchiveBox/ArchiveBox/issues/239. As a mitigation for this issue would be to disable the wget extractor by setting `archivebox config --set SAVE_WGET=False`, ensure you are always logged out, or serve only a [static HTML version] (https://github.com/ArchiveBox/ArchiveBox/wiki/Publishing-Your-Archive#2-export-and-host-it-as-static-html) of your archive.	6.4	More Details
CVE-2023-5615	The Skype Legacy Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'skype-status' shortcode in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-38722	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262174.	6.4	More Details
CVE-2023-5337	The Contact form Form For All plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'formforall' shortcode in versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5292	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'acfe_form' shortcode in versions up to, and including, 0.8.9.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5231	The Magic Action Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.17.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5618	The Modern Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode in versions up to, and including, 1.4.16 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4482	The Auto Amazon Links plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the style parameter in versions up to, and including, 5.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5614	The Theme Switcha plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'theme_switcha_list' shortcode in all versions up to, and including, 3.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5613	The Super Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tpsscode' shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5109	The WP Mailto Links – Protect Email Addresses plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wpml_mailto' shortcode in versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 3.1.3 and fully patched in version 3.1.4.	6.4	More Details
CVE-2023-5086	The Copy Anything to Clipboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'copy' shortcode in versions up to, and including, 2.6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-28797	Zscaler Client Connector for Windows before 4.1 writes/deletes a configuration file inside specific folders on the disk. A malicious user can replace the folder and execute code as a privileged user.	6.3	More Details
CVE-2021-4335	The Fancy Product Designer plugin for WordPress is vulnerable to unauthorized access to data and modification of plugin settings due to a missing capability check on multiple AJAX functions in versions up to, and including, 4.6.9. This makes it possible for authenticated attackers with subscriber-level permissions to modify plugin settings, including retrieving arbitrary order information or creating/updating/deleting products, orders, or other sensitive information not associated with their own account.	6.3	More Details
CVE-2023-5683	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20231010 and classified as critical. This issue affects some unknown processing of the file /sysmanage/importconf.php. The manipulation of the argument btn_file_renew leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5693	A vulnerability was found in CodeAstro Internet Banking System 1.0 and classified as critical. This issue affects some unknown processing of the file pages_reset_pwd.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243131.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41088	The affected product is vulnerable to a cleartext transmission of sensitive information vulnerability, which may allow an attacker with access to the network, where clients have access to the DexGate server, could capture traffic. The attacker can later us the information within it to access the application.	6.3	More Details
CVE-2023-3933	The Your Journey theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.9.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-38192	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows superadmincreate.php XSS via crafted incorrect passwords.	6.1	More Details
CVE-2023-46287	XSS exists in NagVis before 1.9.38 via the select function in share/server/core/functions/html.php.	6.1	More Details
CVE-2023-38194	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows keepalive.php XSS via a GET parameter.	6.1	More Details
CVE-2023-3962	The Winters theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.4.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-4635	The EventON plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 2.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-3965	The nsc theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38191	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows spamtest_external.php XSS via a crafted filename.	6.1	More Details
CVE-2021-46898	views/switch.py in django-grappelli (aka Django Grappelli) before 2.15.2 attempts to prevent external redirection with startswith("/") but this does not consider a protocol-relative URL (e.g., //example.com) attack.	6.1	More Details
CVE-2023-5631	Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code.	6.1	More Details
CVE-2023-45819	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's Notification Manager API. The vulnerability exploits TinyMCE's unfiltered notification system, which is used in error handling. The conditions for this exploit requires carefully crafted malicious content to have been inserted into the editor and a notification to have been triggered. When a notification was opened, the HTML within the text argument was displayed unfiltered in the notification. The vulnerability allowed arbitrary JavaScript execution when an notification presented in the TinyMCE UI for the current user. This issue could also be exploited by any integration which uses a TinyMCE notification to display unfiltered HTML content. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring that the HTML displayed in the notification is sanitized, preventing the exploit. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2023-43875	Multiple Cross-Site Scripting (XSS) vulnerabilities in installation of Subrion CMS v.4.2.1 allows a local attacker to execute arbitrary web scripts via a crafted payload injected into the dbhost, dbname, dbuser, adminusername and adminemail.	6.1	More Details
CVE-2023-43341	Cross-site scripting (XSS) vulnerability in evolution evo v.3.2.3 allows a local attacker to execute arbitrary code via a crafted payload injected uid parameter.	6.1	More Details
CVE-2023-45281	An issue in Yamcs 5.8.6 allows attackers to obtain the session cookie via upload of crafted HTML file.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45909	zzzcms v2.2.0 was discovered to contain an open redirect vulnerability.	6.1	More Details
CVE-2023-45958	Thirty Bees Core v1.4.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the backup_pagination parameter at /controller/AdminController.php. This vulnerability allows attackers to execute arbitrary JavaScript in the web browser of a user via a crafted payload.	6.1	More Details
CVE-2023-43801	Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint `/v2/pkgs/tools/installed` and the way it handles plugin names supplied as user input. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can delete arbitrary files or folders belonging to the user that runs the Arduino Create Agent via a crafted HTTP DELETE request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this issue.	6.1	More Details
CVE-2023-43803	Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint `/v2/pkgs/tools/installed` and the way it handles plugin names supplied as user input. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can delete arbitrary files or folders belonging to the user that runs the Arduino Create Agent via a crafted HTTP POST request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2023-45818	TinyMCE is an open source rich text editor. A mutation cross-site scripting (mXSS) vulnerability was discovered in TinyMCE's core undo and redo functionality. When a carefully-crafted HTML snippet passes the XSS sanitisation layer, it is manipulated as a string by internal trimming functions before being stored in the undo stack. If the HTML snippet is restored from the undo stack, the combination of the string manipulation and reparative parsing by either the browser's native [DOMParser API] (https://developer.mozilla.org/en-US/docs/Web/API/DOMParser) (TinyMCE 6) or the SaxParser API (TinyMCE 5) mutates the HTML maliciously, allowing an XSS payload to be executed. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring HTML is trimmed using node-level manipulation instead of string manipulation. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45057	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Hitsteps Web Analytics plugin <= 5.86 versions.	5.9	More Details
CVE-2023-43045	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 could allow a remote user to perform unauthorized actions due to improper authentication. IBM X-Force ID: 266896.	5.9	More Details
CVE-2023-45073	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Michael Koch Mendeley Plugin plugin <= 1.3.2 versions.	5.9	More Details
CVE-2023-45604	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Scott Reilly Get Custom Field Values plugin <= 4.0.1 versions.	5.9	More Details
CVE-2023-45056	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in 100plugins Open User Map plugin <= 1.3.26 versions.	5.9	More Details
CVE-2023-45051	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Image vertical reel scroll slideshow plugin <= 9.0 versions.	5.9	More Details
CVE-2023-38275	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in container images which could lead to further attacks against the system. IBM X-Force ID: 260730.	5.9	More Details
CVE-2023-45802	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.	5.9	More Details
CVE-2023-38276	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in environment variables which could aid in further attacks against the system. IBM X-Force ID: 260736.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45072	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kardi Order auto complete for WooCommerce plugin <= 1.2.0 versions.	5.9	More Details
CVE-2022-24404	Lack of cryptographic integrity check on TETRA air-interface encrypted traffic. Since a stream cipher is employed, this allows an active adversary to manipulate cleartext data in a bit-by-bit fashion.	5.9	More Details
CVE-2023-28803	An authentication bypass by spoofing of a device with a synthetic IP address is possible in Zscaler Client Connector on Windows, allowing a functionality bypass. This issue affects Client Connector: before 3.9.	5.9	More Details
CVE-2023-45008	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPJohnny Comment Reply Email plugin <= 1.0.3 versions.	5.9	More Details
CVE-2023-45820	Directus is a real-time API and App dashboard for managing SQL database content. In affected versions any Directus installation that has websockets enabled can be crashed if the websocket server receives an invalid frame. A malicious user could leverage this bug to crash Directus. This issue has been addressed in version 10.6.2. Users are advised to upgrade. Users unable to upgrade should avoid using websockets.	5.9	More Details
CVE-2023-37532	HCL Commerce Remote Store server could allow a remote attacker, using a specially-crafted URL, to read arbitrary files on the system.	5.8	More Details
CVE-2023-38735	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a victim to a phishing site. IBM X-Force ID: 262482.	5.7	More Details
CVE-2023-45825	ydb-go-sdk is a pure Go native and database/sql driver for the YDB platform. Since ydb-go-sdk v3.48.6 if you use a custom credentials object (implementation of interface Credentials it may leak into logs. This happens because this object could be serialized into an error message using `fmt.Errorf("something went wrong (credentials: %q)", credentials)` during connection to the YDB server. If such logging occurred, a malicious user with access to logs could read sensitive information (i.e. credentials) information and use it to get access to the database. ydb-go-sdk contains this problem in versions from v3.48.6 to v3.53.2. The fix for this problem has been released in version v3.53.3. Users are advised to upgrade. Users unable to upgrade should implement the `fmt.Stringer` interface in your custom credentials type with explicit stringify of object state.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5682	A vulnerability has been found in Tongda OA 2017 and classified as critical. This vulnerability affects unknown code of the file general/hr/training/record/delete.php. The manipulation of the argument RECORD_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-243058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2021-26737	The Zscaler Client Connector for macOS prior to 3.6 did not sufficiently validate RPC clients. A local adversary without sufficient privileges may be able to shutdown the Zscaler tunnel by exploiting a race condition.	5.5	More Details
CVE-2023-42435	The affected product is vulnerable to a cross-site request forgery vulnerability, which may allow an attacker to perform actions with the permissions of a victim user.	5.5	More Details
CVE-2022-4954	The Waiting: One-click countdowns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown name in versions up to, and including, 0.6.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2023-46332	WebAssembly wabt 1.0.33 contains an Out-of-Bound Memory Write in DataSegment::Drop(), which lead to segmentation fault.	5.5	More Details
CVE-2023-43624	CX-Designer Ver.3.740 and earlier (included in CX-One CXONE-AL[][]D-V4) contains an improper restriction of XML external entity reference (XXE) vulnerability. If a user opens a specially crafted project file created by an attacker, sensitive information in the file system where CX-Designer is installed may be disclosed.	5.5	More Details
CVE-2023-43065	Dell Unity prior to 5.3 contains a Cross-site scripting vulnerability. A low-privileged authenticated attacker can exploit these issues to obtain escalated privileges.	5.5	More Details
CVE-2023-4968	The WPLegalPages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wplegalpage' shortcode in versions up to, and including, 2.9.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46331	WebAssembly wabt 1.0.33 has an Out-of-Bound Memory Read in in DataSegment::IsValidRange(), which lead to segmentation fault.	5.5	More Details
CVE-2023-5700	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /protocol/iscgwtunnel/uploadiscgwrouteconf.php. The manipulation of the argument GWLinkId leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243138 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-43356	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Global Meatadata parameter in the Global Settings Menu component.	5.4	More Details
CVE-2023-43353	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the extra parameter in the news menu component.	5.4	More Details
CVE-2023-43354	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Profiles parameter in the Extensions -MicroTiny WYSIWYG editor component.	5.4	More Details
CVE-2023-43355	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the password and password again parameters in the My Preferences - Add user component.	5.4	More Details
CVE-2023-45471	The QAD Search Server is vulnerable to Stored Cross-Site Scripting (XSS) in versions up to, and including, 1.0.0.315 due to insufficient checks on indexes. This makes it possible for unauthenticated attackers to create a new index and inject a malicious web script into its name, that will execute whenever a user accesses the search page.	5.4	More Details
CVE-2023-43357	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Title parameter in the Manage Shortcuts component.	5.4	More Details
CVE-2023-46095	Cross-Site Request Forgery (CSRF) vulnerability in Chetan Gole Smooth Scroll Links [SSL] plugin <= 1.1.0 versions.	5.4	More Details
CVE-2023-37636	A stored cross-site scripting (XSS) vulnerability in UVDesk Community Skeleton v1.1.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Message field when creating a ticket.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46127	Frappe is a full-stack web application framework that uses Python and MariaDB on the server side and an integrated client side library. A malicious Frappe user with desk access could create documents containing HTML payloads allowing HTML Injection. This vulnerability has been patched in version 14.49.0.	5.4	More Details
CVE-2023-45280	Yamcs 5.8.6 allows XSS (issue 2 of 2). It comes with a Bucket as its primary storage mechanism. Buckets allow for the upload of any file. There's a way to upload an HTML file containing arbitrary JavaScript and then navigate to it. Once the user opens the file, the browser will execute the arbitrary JavaScript.	5.4	More Details
CVE-2023-36857	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a replay vulnerability which could allow an attacker to replay older captured packets of traffic to the device to gain access.	5.4	More Details
CVE-2023-45394	Stored Cross-Site Scripting (XSS) vulnerability in the Company field in the "Request a Quote" Section of Small CRM v3.0 allows an attacker to store and execute malicious javascript code in the Admin panel which leads to Admin account takeover.	5.4	More Details
CVE-2023-43346	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the Backend - Dashboard parameter in the Languages Menu component.	5.4	More Details
CVE-2023-40153	The affected product is vulnerable to a cross-site scripting vulnerability, which could allow an attacker to access the web application to introduce arbitrary Java Script by injecting an XSS payload into the 'hostname' parameter of the vulnerable software.	5.4	More Details
CVE-2023-46078	Cross-Site Request Forgery (CSRF) vulnerability in PluginEver WC Serial Numbers plugin <= 1.6.3 versions.	5.4	More Details
CVE-2023-45279	Yamcs 5.8.6 allows XSS (issue 1 of 2). It comes with a Bucket as its primary storage mechanism. Buckets allow for the upload of any file. There's a way to upload a display referencing a malicious JavaScript file to the bucket. The user can then open the uploaded display by selecting Telemetry from the menu and navigating to the display.	5.4	More Details
CVE-2023-4923	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_delete function. This makes it possible for unauthenticated attackers to delete products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43359	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Page Specific Metadata and Smarty data parameters in the Content Manager Menu component.	5.4	More Details
CVE-2023-43344	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the SEO - Meta description parameter in the Pages Menu component.	5.4	More Details
CVE-2023-43342	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the Languages Menu component.	5.4	More Details
CVE-2023-46003	I-doit pro 25 and below is vulnerable to Cross Site Scripting (XSS) via index.php.	5.4	More Details
CVE-2023-4924	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to missing capability checks on the woobe_bulkoperations_delete function. This makes it possible for authenticated attackers, with subscriber access or higher, to delete products.	5.4	More Details
CVE-2023-45821	Artifact Hub is a web-based application that enables finding, installing, and publishing packages and configurations for CNCF projects. During a security audit of Artifact Hub's code base a security researcher identified a bug in which the `registryIsDockerHub` function was only checking that the registry domain had the `docker.io` suffix. Artifact Hub allows providing some Docker credentials that are used to increase the rate limit applied when interacting with the Docker Hub registry API to read publicly available content. Due to the incorrect check described above, it'd be possible to hijack those credentials by purchasing a domain which ends with `docker.io` and deploying a fake OCI registry on it. <https://artifacthub.io/> uses some credentials that only have permissions to read public content available in the Docker Hub. However, even though credentials for private repositories (disabled on `artifacthub.io`) are handled in a different way, other Artifact Hub deployments could have been using them for a different purpose. This issue has been resolved in version `1.16.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2023-46054	Cross Site Scripting (XSS) vulnerability in WBCE CMS v.1.6.1 and before allows a remote attacker to escalate privileges via a crafted script to the website_footer parameter in the admin/settings/save.php component.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5688	Cross-site Scripting (XSS) - DOM in GitHub repository modoboa/modoboa prior to 2.2.2.	5.4	More Details
CVE-2023-5689	Cross-site Scripting (XSS) - DOM in GitHub repository modoboa/modoboa prior to 2.2.2.	5.4	More Details
CVE-2023-43358	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Title parameter in the News Menu component.	5.4	More Details
CVE-2023-4926	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulk_delete_products function. This makes it possible for unauthenticated attackers to delete products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-45998	kodbox 1.44 is vulnerable to Cross Site Scripting (XSS). Customizing global HTML results in storing XSS.	5.4	More Details
CVE-2023-4668	The Ad Inserter for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.7.30 via the ai-debug-processing-fe URL parameter. This can allow unauthenticated attackers to extract sensitive data including installed plugins (present and active), active theme, various plugin settings, WordPress version, as well as some server settings such as memory limit, installation paths.	5.3	More Details
CVE-2023-45682	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds read in `DECODE` macro when `var` is negative. As it can be seen in the definition of `DECODE_RAW` a negative `var` is a valid value. This issue may be used to leak internal memory allocation information.	5.3	More Details
CVE-2023-4645	The Ad Inserter for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.7.30 via the ai_ajax function. This can allow unauthenticated attackers to extract sensitive data such as post titles and slugs (including those of protected posts along with their passwords), usernames, available roles, the plugin license key provided the remote debugging option is enabled. In the default state it is disabled.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45680	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory allocation failure in `start_decoder`. In that case the function returns early, the `f->comment_list` is set to `NULL`, but `f->comment_list_length` is not reset. Later in `vorbis_deinit` it tries to dereference the `NULL` pointer. This issue may lead to denial of service.	5.3	More Details
CVE-2023-45814	Bunkum is an open-source protocol-agnostic request server for custom game servers. First, a little bit of background. So, in the beginning, Bunkum's `AuthenticationService` only supported injecting `IUser`s. However, as Refresh and SoundShapesServer implemented permissions systems support for injecting `IToken`s into endpoints was added. All was well until 4.0. Bunkum 4.0 then changed to enforce relations between `IToken`s and `IUser`s. This wasn't implemented in a very good way in the `AuthenticationService`, and ended up breaking caching in such a way that cached tokens would persist after the lifetime of the request - since we tried to cache both tokens and users. From that point until now, from what I understand, Bunkum was attempting to use that cached token at the start of the next request once cached. Naturally, when that token expired, downstream projects like Refresh would remove the object from Realm - and cause the object in the cache to be in a detached state, causing an exception from invalid use of `IToken.User`. So in other words, a use-after-free since Realm can't manage the lifetime of the cached token. Security-wise, the scope is fairly limited, can only be pulled off on a couple endpoints given a few conditions, and you can't guarantee which token you're going to get. Also, the token *would* get invalidated properly if the endpoint had either a `IToken` usage or a `IUser` usage. The fix is to just wipe the token cache after the request was handled, which is now in `4.2.1`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2021-4353	The WooCommerce Dynamic Pricing and Discounts plugin for WordPress is vulnerable to unauthenticated settings export in versions up to, and including, 2.4.1. This is due to missing authorization on the export() function which makes makes it possible for unauthenticated attackers to export the plugin's settings.	5.3	More Details
CVE-2023-45667	stb_image is a single file MIT licensed library for processing images. If `stbi__load_gif_main` in `stbi_load_gif_from_memory` fails it returns a null pointer and may keep the `z` variable uninitialized. In case the caller also sets the flip vertically flag, it continues and calls `stbi__vertical_flip_slices` with the null pointer result value and the uninitialized `z` value. This may result in a program crash.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5254	The ChatBot plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.8.9 via the qcld_wb_chatbot_check_user function. This can allow unauthenticated attackers to extract sensitive data including confirmation as to whether a user name exists on the site as well as order information for existing users.	5.3	More Details
CVE-2023-45663	stb_image is a single file MIT licensed library for processing images. The stbi__getn function reads a specified number of bytes from context (typically a file) into the specified buffer. In case the file stream points to the end, it returns zero. There are two places where its return value is not checked: In the `stbi__hdr_load` function and in the `stbi__tga_load` function. The latter of the two is likely more exploitable as an attacker may also control the size of an uninitialized buffer.	5.3	More Details
CVE-2023-5533	The AI ChatBot plugin for WordPress is vulnerable to unauthorized use of AJAX actions due to missing capability checks on the corresponding functions in versions up to, and including, 4.8.9 as well as 4.9.2. This makes it possible for unauthenticated attackers to perform some of those actions that were intended for higher privileged users.	5.3	More Details
CVE-2023-3869	The wpDiscuz plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the voteOnComment function in versions up to, and including, 7.6.3. This makes it possible for unauthenticated attackers to increase or decrease the rating of a comment.	5.3	More Details
CVE-2023-42666	The affected product is vulnerable to an exposure of sensitive information to an unauthorized actor vulnerability, which may allow an attacker to create malicious requests for obtaining the information of the version about the web server used.	5.3	More Details
CVE-2023-30633	An issue was discovered in TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report false TPM PCR values, and thus mask malware activity. Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This requires physical access to a target victim's device, or compromise of user credentials for a device. This issue is similar to CVE-2021-42299 (on Surface Pro devices).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3998	The wpDiscuz plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the userRate function in versions up to, and including, 7.6.3. This makes it possible for unauthenticated attackers to increase or decrease the rating of a post.	5.3	More Details
CVE-2023-41894	Home assistant is an open source home automation. The assessment verified that webhooks available in the webhook component are triggerable via the `*.ui.nabu.casa` URL without authentication, even when the webhook is marked as Only accessible from the local network. This issue is facilitated by the SniTun proxy, which sets the source address to 127.0.0.1 on all requests sent to the public URL and forwarded to the local Home Assistant. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-39731	The leakage of the client secret in Kaibutsunosato v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages.	5.3	More Details
CVE-2023-4939	The SALESmanago plugin for WordPress is vulnerable to Log Injection in versions up to, and including, 3.2.4. This is due to the use of a weak authentication token for the /wp-json/salesmanago/v1/callbackApiV3 API endpoint which is simply a SHA1 hash of the site URL and client ID found in the page source of the website. This makes it possible for unauthenticated attackers to inject arbitrary content into the log files, and when combined with another vulnerability this could have significant consequences.	5.3	More Details
CVE-2023-43340	Cross-site scripting (XSS) vulnerability in evolution v.3.2.3 allows a local attacker to execute arbitrary code via a crafted payload injected into the cmsadmin, cmsadminemail, cmspassword and cmspasswordconfim parameters	5.2	More Details
CVE-2023-43074	Dell Unity 5.3 contain(s) an Arbitrary File Creation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by crafting arbitrary files through a request to the server.	5.2	More Details
CVE-2023-43066	Dell Unity prior to 5.3 contains a Restricted Shell Bypass vulnerability. This could allow an authenticated, local attacker to exploit this vulnerability by authenticating to the device CLI and issuing certain commands.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34050	In spring AMQP versions 1.0.0 to 2.4.16 and 3.0.0 to 3.0.9 , allowed list patterns for deserializable class names were added to Spring AMQP, allowing users to lock down deserialization of data in messages from untrusted sources; however by default, when no allowed list was provided, all classes could be deserialized. Specifically, an application is vulnerable if * the SimpleMessageConverter or SerializerMessageConverter is used * the user does not configure allowed list patterns * untrusted message originators gain permissions to write messages to the RabbitMQ broker to send malicious content	5.0	More Details
CVE-2023-43067	Dell Unity prior to 5.3 contains an XML External Entity injection vulnerability. An XXE attack could potentially exploit this vulnerability disclosing local files in the file system.	4.9	More Details
CVE-2023-44760	Multiple Cross Site Scripting (XSS) vulnerabilities in Concrete CMS v.9.2.1 allow an attacker to execute arbitrary code via a crafted script to the Header and Footer Tracking Codes of the SEO & Statistics. NOTE: the vendor disputes this because these header/footer changes can only be made by an admin, and allowing an admin to place JavaScript there is an intentional customization feature. Also, the exploitation method claimed by "sromanhu" does not provide any access to a Concrete CMS session, because the Concrete CMS session cookie is configured as HttpOnly.	4.8	More Details
CVE-2023-33840	IBM Security Verify Governance 10.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256037.	4.8	More Details
CVE-2023-27149	A stored cross-site scripting (XSS) vulnerability in Enhancesoft osTicket v1.17.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Label input parameter when updating a custom list.	4.8	More Details
CVE-2023-46058	Cross Site Scripting (XSS) vulnerability in Geeklog-Core geeklog v.2.2.2 allows a remote attacker to execute arbitrary code via a crafted payload to the grp_desc parameter of the admin/group.php component.	4.8	More Details
CVE-2023-27148	A stored cross-site scripting (XSS) vulnerability in the Admin panel in Enhancesoft osTicket v1.17.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Role Name parameter.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46059	Cross Site Scripting (XSS) vulnerability in Geeklog-Core geeklog v.2.2.2 allows a remote attacker to execute arbitrary code via a crafted payload to the Service, and website URL to Ping parameters of the admin/trackback.php component.	4.8	More Details
CVE-2023-5684	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20231012. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /importexport.php. The manipulation leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243061 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-5681	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/list_addr_fwresource_ip.php. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243057 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2022-3622	The Blog2Social plugin for WordPress is vulnerable to authorization bypass due to missing capability checks in versions up to, and including, 6.9.11. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to change some plugin settings intended to be modifiable by admins only.	4.7	More Details
CVE-2023-45813	Torbot is an open source tor network intelligence tool. In affected versions the `torbot.modules.validators.validate_link function` uses the python-validators URL validation regex. This particular regular expression has an exponential complexity which allows an attacker to cause an application crash using a well-crafted argument. An attacker can use a well-crafted URL argument to exploit the vulnerability in the regular expression and cause a Denial of Service on the system. The validators file has been removed in version 4.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.6	More Details
CVE-2023-32087	Pega Platform versions 8.1 to Infinity 23.1.0 are affected by an XSS issue with task creation	4.6	More Details
CVE-2023-32088	Pega Platform versions 8.1 to Infinity 23.1.0 are affected by an XSS issue with ad-hoc case creation	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32089	Pega Platform versions 8.1 to 8.8.2 are affected by an XSS issue with Pin description	4.6	More Details
CVE-2023-4271	The Photospace Responsive plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'psres_button_size' parameter in versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2021-26734	Zscaler Client Connector Installer on Windows before version 3.4.0.124 improperly handled directory junctions during uninstallation. A local adversary may be able to delete folders in an elevated context.	4.4	More Details
CVE-2023-5121	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings (the backup path parameter) in versions up to, and including, 0.9.89 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-3996	The ARMember Lite - Membership Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 4.0.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-5120	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the image file path parameter in versions up to, and including, 0.9.89 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25332	The AES implementation in the Texas Instruments OMAP L138 (secure variants), present in mask ROM, suffers from a timing side channel which can be exploited by an adversary with non-secure supervisor privileges by managing cache contents and collecting timing information for different ciphertext inputs. Using this side channel, the SK_LOAD secure kernel routine can be used to recover the Customer Encryption Key (CEK).	4.4	More Details
CVE-2023-4648	The WP Customer Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 3.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-5621	The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Title field in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-4021	The Modern Events Calendar lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Google API key and Calendar ID in versions up to, but not including, 7.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-4943	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_visibility function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products.	4.3	More Details
CVE-2023-4940	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_swap function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4947	The WooCommerce EAN Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the refresh_order_ean_data AJAX action in versions up to 6.1.0. This makes it possible for authenticated attackers with contributor-level access and above, to update EAN numbers for orders.	4.3	More Details
CVE-2023-4975	The Website Builder by SeedProd plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.15.13.1. This is due to missing or incorrect nonce validation on functionality in the builder.php file. This makes it possible for unauthenticated attackers to change the stripe connect token via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-4920	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_save_options function. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Additionally, input sanitization and escaping is insufficient resulting in the possibility of malicious script injection.	4.3	More Details
CVE-2023-4937	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_apply_default_combination function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-5718	The Vue.js Devtools extension was found to leak screenshot data back to a malicious web page via the standard `postMessage()` API. By creating a malicious web page with an iFrame targeting a sensitive resource (i.e. a locally accessible file or sensitive website), and registering a listener on the web page, the extension sent messages back to the listener, containing the base64 encoded screenshot data of the sensitive resource.	4.3	More Details
CVE-2023-4935	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the create_profile function. This makes it possible for unauthenticated attackers to create profiles via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36751	The Coupon Creator plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.1. This is due to missing or incorrect nonce validation on the save_meta() function. This makes it possible for unauthenticated attackers to save meta fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-46288	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Airflow.This issue affects Apache Airflow from 2.4.0 to 2.7.0. Sensitive configuration information has been exposed to authenticated users with the ability to read configuration via Airflow REST API for configuration even when the expose_config option is set to non-sensitive-only. The expose_config option is False by default. It is recommended to upgrade to a version that is not affected if you set expose_config to non-sensitive-only configuration. This is a different error than CVE-2023-45348 which allows authenticated user to retrieve individual configuration values in 2.7.* by specially crafting their request (solved in 2.7.2). Users are recommended to upgrade to version 2.7.2, which fixes the issue and additionally fixes CVE-2023-45348.	4.3	More Details
CVE-2023-41893	Home assistant is an open source home automation. The audit team's analyses confirmed that the `redirect_uri` and `client_id` are alterable when logging in. Consequently, the code parameter utilized to fetch the `access_token` post-authentication will be sent to the URL specified in the aforementioned parameters. Since an arbitrary URL is permitted and `homeassistant.local` represents the preferred, default domain likely used and trusted by many users, an attacker could leverage this weakness to manipulate a user and retrieve account access. Notably, this attack strategy is plausible if the victim has exposed their Home Assistant to the Internet, since after acquiring the victim's `access_token` the adversary would need to utilize it directly towards the instance to achieve any pertinent malicious actions. To achieve this compromise attempt, the attacker must send a link with a `redirect_uri` that they control to the victim's own Home Assistant instance. In the eventuality the victim authenticates via said link, the attacker would obtain code sent to the specified URL in `redirect_uri`, which can then be leveraged to fetch an `access_token`. Pertinently, an attacker could increase the efficacy of this strategy by registering a near identical domain to `homeassistant.local`, which at first glance may appear legitimate and thereby obfuscate any malicious intentions. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4938	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_apply_default_combination function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products.	4.3	More Details
CVE-2023-3254	The Widgets for Google Reviews plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 10.9. This is due to missing or incorrect nonce validation within setup_no_reg_header.php. This makes it possible for unauthenticated attackers to reset plugin settings and remove reviews via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-46089	Cross-Site Request Forgery (CSRF) vulnerability in Lee Le @ Userback Userback plugin <= 1.0.13 versions.	4.3	More Details
CVE-2023-46085	Cross-Site Request Forgery (CSRF) vulnerability in Wpmet Wp Ultimate Review plugin <= 2.2.4 versions.	4.3	More Details
CVE-2020-36753	The Hueman theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.6.3. This is due to missing or incorrect nonce validation on the save_meta_box() function. This makes it possible for unauthenticated attackers to save metabox data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-5702	A vulnerability was found in Viessmann Vitogate 300 up to 2.1.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/. The manipulation leads to direct request. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-46067	Cross-Site Request Forgery (CSRF) vulnerability in Qwerty23 Rocket Font plugin <= 1.2.3 versions.	4.3	More Details
CVE-2020-36754	The Paid Memberships Pro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4.2. This is due to missing or incorrect nonce validation on the pmpro_page_save() function. This makes it possible for unauthenticated attackers to save pages via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5602	The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.5. This is due to missing or incorrect nonce validation on several functions corresponding to AJAX actions. This makes it possible for unauthenticated attackers to invoke those actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-5534	The AI ChatBot plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.8.9 and 4.9.2. This is due to missing or incorrect nonce validation on the corresponding functions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-5701	A vulnerability has been found in vnotex vnote up to 3.17.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Markdown File Handler. The manipulation with the input <xss onclick="alert(1)" style=display:block>Click here</xss> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243139. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4942	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_visibility function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-4941	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_swap function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products.	4.3	More Details
CVE-2020-36755	The Customizr theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.3.0. This is due to missing or incorrect nonce validation on the czr_fn_post_fields_save() function. This makes it possible for unauthenticated attackers to post fields via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4796	The Booster for WooCommerce for WordPress is vulnerable to Information Disclosure via the 'wcj_wp_option' shortcode in versions up to, and including, 7.1.0 due to insufficient controls on the information retrievable via the shortcode. This makes it possible for authenticated attackers, with subscriber-level capabilities or above, to retrieve arbitrary sensitive site options.	4.3	More Details
CVE-2020-36758	The RSS Aggregator by Feedzy plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4.2. This is due to missing or incorrect nonce validation on the save_feedzy_post_type_meta() function. This makes it possible for unauthenticated attackers to update post meta via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-36759	The Woody code snippets plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.3.9. This is due to missing or incorrect nonce validation on the runActions() function. This makes it possible for unauthenticated attackers to activate and deactivate snippets via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2021-4418	The Custom CSS, JS & PHP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0.7. This is due to missing or incorrect nonce validation on the save() function. This makes it possible for unauthenticated attackers to save code snippets via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-33837	IBM Security Verify Governance 10.0 does not encrypt sensitive or critical information before storage or transmission. IBM X-Force ID: 256020.	4.1	More Details
CVE-2023-46122	sbt is a build tool for Scala, Java, and others. Given a specially crafted zip or JAR file, `IO.unzip` allows writing of arbitrary file. This would have potential to overwrite `/root/.ssh/authorized_keys`. Within sbt's main code, `IO.unzip` is used in `pullRemoteCache` task and `Resolvers.remote`; however many projects use `IO.unzip(...)` directly to implement custom tasks. This vulnerability has been patched in version 1.9.7.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38546	This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met. libcurl performs transfers. In its API, an application creates "easy handles" that are the individual handles for single transfers. libcurl provides a function call that duplicates en easy handle called [curl_easy_duphandle](https://curl.se/libcurl/c/curl_easy_duphandle.html). If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as `none` (using the four ASCII letters, no quotes). Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named `none` - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.	3.7	More Details
CVE-2023-45822	Artifact Hub is a web-based application that enables finding, installing, and publishing packages and configurations for CNCF projects. During a security audit of Artifact Hub's code base a security researcher identified a bug in which a default unsafe rego built-in was allowed to be used when defining authorization policies. Artifact Hub includes a fine-grained authorization mechanism that allows organizations to define what actions can be performed by their members. It is based on customizable authorization policies that are enforced by the `Open Policy Agent`. Policies are written using `rego` and their data files are expected to be json documents. By default, `rego` allows policies to make HTTP requests, which can be abused to send requests to internal resources and forward the responses to an external entity. In the context of Artifact Hub, this capability should have been disabled. This issue has been resolved in version `1.16.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.7	More Details
CVE-2023-45145	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory.	3.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5694	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been classified as problematic. Affected is an unknown function of the file pages_system_settings.php. The manipulation of the argument sys_name with the input <ScRiPt >alert(991)</ScRiPt> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243132.	3.5	More Details
CVE-2023-5695	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file pages_reset_pwd.php. The manipulation of the argument email with the input testing%40example.com'%26%25<ScRiPt%20>alert(9860)</ScRiPt> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243133 was assigned to this vulnerability.	3.5	More Details
CVE-2023-5699	A vulnerability, which was classified as problematic, has been found in CodeAstro Internet Banking System 1.0. This issue affects some unknown processing of the file pages_view_client.php. The manipulation of the argument acc_name with the input Johnnie Reyes'"()&%<zzz> <ScRiPt >alert(5646)</ScRiPt> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243137 was assigned to this vulnerability.	3.5	More Details
CVE-2023-5696	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file pages_transfer_money.php. The manipulation of the argument account_number with the input 357146928--> <ScRiPt%20>alert(9206)</ScRiPt><!-- leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-243134 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-5698	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. This vulnerability affects unknown code of the file pages_deposit_money.php. The manipulation of the argument account_number with the input 421873905--><ScRiPt%20>alert(9523) </ScRiPt><!-- leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243136.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5697	A vulnerability classified as problematic has been found in CodeAstro Internet Banking System 1.0. This affects an unknown part of the file pages_withdraw_money.php. The manipulation of the argument account_number with the input 287359614--><ScRiPt%20>alert(1234)</ScRiPt><!-- leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243135.	3.5	More Details
CVE-2023-45809	Wagtail is an open source content management system built on Django. A user with a limited-permission editor account for the Wagtail admin can make a direct URL request to the admin view that handles bulk actions on user accounts. While authentication rules prevent the user from making any changes, the error message discloses the display names of user accounts, and by modifying URL parameters, the user can retrieve the display name for any user. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 4.1.8 (LTS), 5.0.5 and 5.1.3. The fix is also included in Release Candidate 1 of the forthcoming Wagtail 5.2 release. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2.7	More Details
CVE-2023-5656	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-5533. Reason: This record is a reservation duplicate of CVE-2023-5533. Notes: All CVE users should reference CVE-2023-5533 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-45665	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2023-5647	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-5212. Reason: This record is a reservation duplicate of CVE-2023-5212. Notes: All CVE users should reference CVE-2023-5212 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-5655	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-5534. Reason: This record is a reservation duplicate of CVE-2023-5534. Notes: All CVE users should reference CVE-2023-5534 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32785	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-36189. Reason: This record is a duplicate of CVE-2023-36189. Notes: All CVE users should reference CVE-2023-36189 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-4531	Rejected reason: Not a valid vulnerability.	N/A	More Details
CVE-2023-46267	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-5631. Reason: This candidate is a duplicate of CVE-2023-5631. Notes: All CVE users should reference CVE-2023-5631 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-5646	Rejected reason: ** REJECT **DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-5241. Reason: This record is a reservation duplicate of CVE-2023-5241. Notes: All CVE users should reference CVE-2023-5241 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details