SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 31 May 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-1424	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series CPU modules and MELSEC iQ-R Series CPU modules allows a remote unauthenticated attacker to cause a denial of service (DoS) condition or execute malicious code on a target product by sending specially crafted packets. A system reset of the product is required for recovery from a denial of service (DoS) condition and malicious code execution.	10.0	More Details
CVE-2023-33189	Pomerium is an identity and context-aware access proxy. With specially crafted requests, incorrect authorization decisions may be made by Pomerium. This issue has been patched in versions 0.17.4, 0.18.1, 0.19.2, 0.20.1, 0.21.4 and 0.22.2.	10.0	More Details
CVE-2023-2825	An issue has been discovered in GitLab CE/EE affecting only version 16.0.0. An unauthenticated malicious user can use a path traversal vulnerability to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups.	10.0	More Details
CVE-2022-48478	The facial recognition TA of some products lacks memory length verification. Successful exploitation of this vulnerability may cause exceptions of the facial recognition service.	9.8	More Details
CVE-2022-48479	The facial recognition TA of some products has the out-of-bounds memory read vulnerability. Successful exploitation of this vulnerability may cause exceptions of the facial recognition service.	9.8	More Details
CVE-2023-32321	CKAN is an open-source data management system for powering data hubs and data portals. Multiple vulnerabilities have been discovered in Ckan which may lead to remote code execution. An arbitrary file write in `resource_create` and `package_update` actions, using the `ResourceUploader` object. Also reachable via `package_create`, `package_revise`, and `package_patch` via calls to `package_update`. Remote code execution via unsafe pickle loading, via Beaker's session store when configured to use the file session store backend. Potential DOS due to lack of a length check on the resource id. Information disclosure: A user with permission to create a resource can access any other resource on the system if they know the id, even if they don't have access to it. Resource overwrite: A user with permission to create a resource can overwrite any resource if they know the id, even if they don't have access to it. A user with permissions to create or edit a dataset can upload a resource with a specially crafted id to write the uploaded file in an arbitrary location. This can be leveraged to Remote Code Execution via Beaker's insecure pickle loading. All the above listed vulnerabilities have been fixed in CKAN 2.9.9 and CKAN 2.10.1. Users are advised to upgrade. There are no known workarounds for these issues.	9.8	More Details
CVE-2015-20108	xml_security.rb in the ruby-saml gem before 1.0.0 for Ruby allows XPath injection and code execution because prepared statements are not used.	9.8	More Details
CVE-2019-19791	In LemonLDAP::NG (aka lemonldap-ng) before 2.0.7, the default Apache HTTP Server configuration does not properly restrict access to SOAP/REST endpoints (when some LemonLDAP::NG setup options are used). For example, an attacker can insert index.fcgi/index.fcgi into a URL to bypass a Require directive.	9.8	More Details
CVE-2022-24627	An issue was discovered in AudioCodes Device Manager Express through 7.8.20002.47752. It is an unauthenticated SQL injection in the p parameter of the process_login.php login form.	9.8	More Details
CVE-2022-24629	An issue was discovered in AudioCodes Device Manager Express through 7.8.20002.47752. Remote code execution can be achieved via directory traversal in the dir parameter of the file upload functionality of BrowseFiles.php. An attacker can upload a .php file to WebAdmin/admin/AudioCodes_files/ajax/.	9.8	More Details
CVE-2023-32692	CodeIgniter is a PHP full-stack web framework. This vulnerability allows attackers to execute arbitrary code when you use Validation Placeholders. The vulnerability exists in the Validation library, and validation methods in the controller and in-model validation are also vulnerable because they use the Validation library internally. This issue is patched in version 4.3.5.	9.8	More Details
CVE-2023-2972	Prototype Pollution in GitHub repository antfu/utils prior to 0.7.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30145	Camaleon CMS v2.7.0 was discovered to contain a Server-Side Template Injection (SSTI) vulnerability via the formats parameter.	9.8	More Details
CVE-2023-33975	RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. In version 2023.01 and prior, an attacker can send a crafted frame to the device resulting in an out of bounds write in the packet buffer. The overflow can be used to corrupt other packets and the allocator metadata. Corrupting a pointer will easily lead to denial of service. While carefully manipulating the allocator metadata gives an attacker the possibility to write data to arbitrary locations and thus execute arbitrary code. This issue is fixed in pull request 19680. As a workaround, disable support for fragmented IP datagrams.	9.8	More Details
CVE-2022-36246	Shop Beat Solutions (Pty) LTD Shop Beat Media Player 2.5.95 up to 3.2.57 is vulnerable to Insecure Permissions.	9.8	More Details
CVE-2023-29732	SoLive 1.6.14 thru 1.6.20 for Android exists exposed component, the component provides the method to modify the SharedPreference file. The attacker can use the method to modify the data in any SharedPreference file, these data will be loaded into the memory when the application is opened. Depending on how the data is used, this can result in various attack consequences, such as ad display exceptions.	9.8	More Details
CVE-2023-29734	An issue found in edjing Mix v.7.09.01 for Android allows unauthorized apps to cause escalation of privilege attacks by manipulating the database.	9.8	More Details
CVE-2023-33734	BlueCMS v1.6 was discovered to contain a SQL injection vulnerability via the keywords parameter at search.php.	9.8	More Details
CVE-2023-34152	A vulnerability was found in ImageMagick. This security flaw cause a remote code execution vulnerability in OpenBlob with --enable-pipes configured.	9.8	More Details
CVE-2023-29727	The Call Blocker application 6.6.3 for Android allows unauthorized applications to use exposed components to delete data stored in its database that is related to user privacy settings and affects the implementation of the normal functionality of the application. An attacker can use this to cause an escalation of privilege attack.	9.8	More Details
CVE-2023-29728	The Call Blocker application 6.6.3 for Android allows attackers to tamper with feature-related data, resulting in a severe elevation of privilege attack.	9.8	More Details
CVE-2023-29739	An issue found in Alarm Clock for Heavy Sleepers v.5.3.2 for Android allows unauthorized apps to cause escalation of privilege attacks by manipulating the component.	9.8	More Details
CVE-2023-2750	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cityboss E-municipality allows SQL Injection.This issue affects E-municipality: before 6.05.	9.8	More Details
CVE-2021-46887	Lack of length check vulnerability in the HW_KEYMASTER module. Successful exploitation of this vulnerability may cause out-of-bounds read.	9.8	More Details
CVE-2023-31458	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect versions 19.3 SP2 (22.24.1500.0) and earlier could allow an unauthenticated attacker with internal network access to authenticate with administrative privileges, because initial installation does not enforce a password change. A successful exploit could allow an attacker to make arbitrary configuration changes and execute arbitrary commands.	9.8	More Details
CVE-2023-2732	The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.2. This is due to insufficient verification on the user being supplied during the add listing REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id.	9.8	More Details
CVE-2023-33009	A buffer overflow vulnerability in the notification function in Zyxel ATP series firmware versions 4.60 through 5.36 Patch 1, USG FLEX series firmware versions 4.60 through 5.36 Patch 1, USG FLEX 50(W) firmware versions 4.60 through 5.36 Patch 1, USG20(W)-VPN firmware versions 4.60 through 5.36 Patch 1, VPN series firmware versions 4.60 through 5.36 Patch 1, ZyWALL/USG series firmware versions 4.60 through 4.73 Patch 1, could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and even a remote code execution on an affected device.	9.8	More Details
CVE-2023-33010	A buffer overflow vulnerability in the ID processing function in Zyxel ATP series firmware versions 4.32 through 5.36 Patch 1, USG FLEX series firmware versions 4.50 through 5.36 Patch 1, USG FLEX 50(W) firmware versions 4.25 through 5.36 Patch 1, USG20(W)-VPN firmware versions 4.25 through 5.36 Patch 1, VPN series firmware versions 4.30 through 5.36 Patch 1, ZyWALL/USG series firmware versions 4.25 through 4.73 Patch 1, could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and even a remote code execution on an affected device.	9.8	More Details
CVE-2023-2045	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ipekyolu Software Auto Damage Tracking Software allows SQL Injection.This issue affects Auto Damage Tracking Software: before 4.	9.8	More Details
CVE-2023-2064	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Minova Technology eTrace allows SQL Injection.This issue affects eTrace: before 23.05.20.	9.8	More Details
CVE-2023-33246	For RocketMQ versions 5.1.0 and below, under certain conditions, there is a risk of remote command execution. Several components of RocketMQ, including NameServer, Broker, and Controller, are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as. Additionally, an attacker can achieve the same effect by forging the RocketMQ protocol content. To prevent these attacks, users are recommended to upgrade to version 5.1.1 or above for using RocketMQ 5.x or 4.9.6 or above for using RocketMQ 4.x .	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1174	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the minikube container.	9.8	More Details
CVE-2023-31457	A vulnerability in the Headquarters server component of Mitel MiVoice Connect versions 19.3 SP2 (22.24.1500.0) and earlier could allow an unauthenticated attacker with internal network access to execute arbitrary scripts due to improper access control.	9.8	More Details
CVE-2023-29721	SofaWiki <= 3.8.9 has a file upload vulnerability that leads to command execution.	9.8	More Details
CVE-2023-33280	In the Store Commander scquickaccounting module for PrestaShop through 3.7.3, multiple sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection.	9.8	More Details
CVE-2023-29741	An issue found in BestWeather v.7.3.1 for Android allows unauthorized apps to cause an escalation of privileges attack by manipulating the database.	9.8	More Details
CVE-2023-2733	The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.0. This is due to insufficient verification on the user being supplied during the coupon redemption REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id.	9.8	More Details
CVE-2023-2734	The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.1. This is due to insufficient verification on the user being supplied during the cart sync from mobile REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id.	9.8	More Details
CVE-2023-2882	Generation of Incorrect Security Tokens vulnerability in CBOT Chatbot allows Token Impersonation, Privilege Abuse.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.	9.8	More Details
CVE-2023-2884	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Use of Insufficiently Random Values vulnerability in CBOT Chatbot allows Signature Spoofing by Key Recreation.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.	9.8	More Details
CVE-2023-2887	Authentication Bypass by Spoofing vulnerability in CBOT Chatbot allows Authentication Bypass.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.	9.8	More Details
CVE-2023-2851	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AGT Tech Ceppatron allows Command Line Execution through SQL Injection, SQL Injection.This issue affects all versions of the sofware also EOS when CVE-ID assigned.	9.8	More Details
CVE-2023-33278	In the Store Commander scexportcustomers module for PrestaShop through 3.6.1, sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection.	9.8	More Details
CVE-2023-33279	In the Store Commander scfixmyprestashop module through 2023-05-09 for PrestaShop, sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection.	9.8	More Details
CVE-2023-2868	A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product effecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user-supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product. This issue was fixed as part of BNSF-36456 patch. This patch was automatically applied to all customer appliances.	9.4	More Details
CVE-2023-34205	In Moov signedxml through 1.0.0, parsing the raw XML (as received) can result in different output than parsing the canonicalized XML. Thus, signature validation can be bypassed via a Signature Wrapping attack (aka XSW).	9.1	More Details
CVE-2023-33175	ToUI is a Python package for creating user interfaces (websites and desktop apps) from HTML. ToUI is using Flask-Caching (SimpleCache) to store user variables. Websites that use `Website.user_vars` property. It affects versions 2.0.1 to 2.4.0. This issue has been patched in version 2.4.1.	9.1	More Details
CVE-2023-33193	Emby Server is a user-installable home media server which stores and organizes a user's media files of virtually any format and makes them available for viewing at home and abroad on a broad range of client devices. This vulnerability may allow administrative access to an Emby Server system, depending on certain user account settings. By spoofing certain headers which are intended for interoperation with reverse proxy servers, it may be possible to affect the local/non-local network determination to allow logging in without password or to view a list of user accounts which may have no password configured. Impacted are all Emby Server system which are publicly accessible and where the administrator hasn't tightened the account login configuration for administrative users. This issue has been patched in Emby Server Beta version 4.8.31 and Emby Server version 4.7.12.	9.1	More Details
CVE-2023-33796	A vulnerability in Netbox v3.5.1 allows unauthenticated attackers to execute queries against the GraphQL database, granting them access to sensitive data stored in the database. NOTE: the vendor disputes this because the reporter's only query was for the schema of the API, which is public; queries for database objects would have been denied.	9.1	More Details
CVE-2022-36247	Shop Beat Solutions (Pty) LTD Shop Beat Media Player 2.5.95 up to 3.2.57 is vulnerable to IDOR via controlpanel.shopbeat.co.za.	9.1	More Details
CVE-2023-26216	The server component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an exploitable vulnerability that allows an attacker to upload files to a directory accessible by the web server. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.5.16 and below.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46945	Nagvis before 1.9.34 was discovered to contain an arbitrary file read vulnerability via the component /core/classes/NagVisHoverUrl.php.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Refer
CVE-2023-33961	Leantime is a lean open source project management system. Starting in version 2.3.21, an authenticated user with commenting privileges can inject malicious Javascript into a comment. Once the malicious comment is loaded in the browser by a user, the malicious Javascript code executes. As of time of publication, a patch does not exist.	8.9	More Detail
CVE-2023-2935	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Detail
CVE-2023-2929	Out of bounds write in Swiftshader in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Detail
CVE-2023-31874	Yank Note (YN) 3.52.1 allows execution of arbitrary code when a crafted file is opened, e.g., via nodeRequire('child_process').	8.8	More Detail
CVE-2023-32696	CKAN is an open-source data management system for powering data hubs and data portals. Prior to versions 2.9.9 and 2.10.1, the `ckan` user (equivalent to www-data) owned code and configuration files in the docker container and the `ckan` user had the permissions to use sudo. These issues allowed for code execution or privilege escalation if an arbitrary file write bug was available. Versions 2.9.9, 2.9.9-dev, 2.10.1, and 2.10.1-dev contain a patch.	8.8	More Detail
CVE-2023-0766	The Newsletter Popup WordPress plugin through 1.2 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks as the wp_newsletter_show_localrecord page is not protected with a nonce.	8.8	More Detail
CVE-2023-2288	The Otter WordPress plugin before 2.2.6 does not sanitize some user-controlled file paths before performing file operations on them. This leads to a PHAR deserialization vulnerability on PHP < 8.0 using the phar:// stream wrapper.	8.8	More Detail
CVE-2023-2936	Type Confusion in V8 in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Detail
CVE-2023-2883	Authorization Bypass Through User-Controlled Key vulnerability in CBOT Chatbot allows Authentication Abuse, Authentication Bypass.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.	8.8	More Detail
CVE-2023-30253	Dolibarr before 17.0.1 allows remote code execution by an authenticated user via an uppercase manipulation: <?PHP instead of <?php in injected data.	8.8	More Detail
CVE-2023-33177	Xibo is a content management system (CMS). A path traversal vulnerability exists in the Xibo CMS whereby a specially crafted zip file can be uploaded to the CMS via the layout import function by an authenticated user which would allow creation of files outside of the CMS library directory as the webserver user. This can be used to upload a PHP webshell inside the web root directory and achieve remote code execution as the webserver user. Users should upgrade to version 2.3.17 or 3.3.5, which fix this issue. Customers who host their CMS with Xibo Signage have already received an upgrade or patch to resolve this issue regardless of the CMS version that they are running.	8.8	More Detail
CVE-2023-2983	Privilege Defined With Unsafe Actions in GitHub repository pimcore/pimcore prior to 10.5.23.	8.8	More Detail
CVE-2023-31459	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect versions 9.6.2208.101 and earlier could allow an unauthenticated attacker with internal network access to authenticate with administrative privileges, because the initial installation does not enforce a password change. A successful exploit could allow an attacker to make arbitrary configuration changes and execute arbitrary commands.	8.8	More Detail
CVE-2023-2984	Path Traversal: '\..\filename' in GitHub repository pimcore/pimcore prior to 10.5.22.	8.8	More Detail
CVE-2023-2930	Use after free in Extensions in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Detail
CVE-2023-2931	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-2065	Authorization Bypass Through User-Controlled Key vulnerability in Armoli Technology Cargo Tracking System allows Authentication Abuse, Authentication Bypass.This issue affects Cargo Tracking System: before 3558f28 .	8.8	More Detail
CVE-2023-2932	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Detail
CVE-2023-2933	Use after free in PDF in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: High)	8.8	More Detail
CVE-2022-36250	Shop Beat Solutions (Pty) LTD Shop Beat Media Player 2.5.95 up to 3.2.57 is vulnerable to Cross Site Request Forgery (CSRF).	8.8	More Detail
CVE-2023-2500	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 3.3.19 via deserialization of untrusted input from the 'go_pricing' shortcode 'data' parameter. This allows authenticated attackers, with subscriber-level permissions and above, 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.	8.8	More Detail
CVE-2023-2859	Code Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.9.	8.8	More Detail
CVE-2023-1938	The WP Fastest Cache WordPress plugin before 1.1.5 does not have CSRF check in an AJAX action, and does not validate user input before using it in the wp_remote_get() function, leading to a Blind SSRF issue	8.8	More Detail
CVE-2023-33245	Minecraft through 1.19 and 1.20 pre-releases before 7 (Java) allow arbitrary file overwrite, and possibly code execution, via crafted world data that contains a symlink.	8.8	More Detail
CVE-2023-2943	Code Injection in GitHub repository openemr/openemr prior to 7.0.1.	8.8	More Detail
CVE-2023-2934	Out of bounds memory access in Mojo in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Detail
CVE-2023-33779	A lateral privilege escalation vulnerability in XXL-Job v2.4.1 allows users to execute arbitrary commands on another user's account via a crafted POST request to the component /jobinfo/.	8.8	More Detail
CVE-2023-30350	FS S3900-24T4S devices allow authenticated attackers with guest access to escalate their privileges and reset the admin password.	8.8	More Detail
CVE-2023-32315	Openfire is an XMPP server licensed under the Open Source Apache License. Openfire's administrative console, a web-based application, was found to be vulnerable to a path traversal attack via the setup environment. This permitted an unauthenticated user to use the unauthenticated Openfire Setup Environment in an already configured Openfire environment to access restricted pages in the Openfire Admin Console reserved for administrative users. This vulnerability affects all versions of Openfire that have been released since April 2015, starting with version 3.10.0. The problem has been patched in Openfire release 4.7.5 and 4.6.8, and further improvements will be included in the yet-to-be released first version on the 4.8 branch (which is expected to be version 4.8.0). Users are advised to upgrade. If an Openfire upgrade isn't available for a specific release, or isn't quickly actionable, users may see the linked github advisory (GHSA-gw42-f939-fhvm) for mitigation advice.	8.6	More Detail
CVE-2023-26128	All versions of the package keep-module-latest are vulnerable to Command Injection due to missing input sanitization or other checks and sandboxes being employed to the installModule function. **Note:** To execute the code snippet and potentially exploit the vulnerability, the attacker needs to have the ability to run Node.js code within the target environment. This typically requires some level of access to the system or application hosting the Node.js environment.	8.4	More Detail
CVE-2023-1944	This vulnerability enables ssh access to minikube container using a default password.	8.4	More Detail
CVE-2023-26129	All versions of the package bwm-ng are vulnerable to Command Injection due to improper input sanitization in the 'check' function in the bwm-ng.js file. **Note:** To execute the code snippet and potentially exploit the vulnerability, the attacker needs to have the ability to run Node.js code within the target environment. This typically requires some level of access to the system or application hosting the Node.js environment.	8.4	More Detail
CVE-2023-33186	Zulip is an open-source team collaboration tool with unique topic-based threading that combines the best of email and chat to make remote work productive and delightful. The main development branch of Zulip Server from May 2, 2023 and later, including beta versions 7.0-beta1 and 7.0-beta2, is vulnerable to a cross-site scripting vulnerability in tooltips on the message feed. An attacker who can send messages could maliciously craft a topic for the message, such that a victim who hovers the tooltip for that topic in their message feed triggers execution of JavaScript code controlled by the attacker.	8.2	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-32686	Kiwi TCMS is an open source test management system for both manual and automated testing. Kiwi TCMS allows users to upload attachments to test plans, test cases, etc. Earlier versions of Kiwi TCMS had introduced upload validators in order to prevent potentially dangerous files from being uploaded. The upload validation checks were not robust enough which left the possibility of an attacker to circumvent them and upload a potentially dangerous file. Exploiting this flaw, a combination of files could be uploaded so that they work together to circumvent the existing Content-Security-Policy and allow execution of arbitrary JavaScript in the browser. This issue has been patched in version 12.3.	8.1	More Detail
CVE-2023-2950	Improper Authorization in GitHub repository openemr/openemr prior to 7.0.1.	8.1	More Detail
CVE-2023-2946	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.1.	8.1	More Detail
CVE-2023-32319	Nextcloud server is an open source personal cloud implementation. Missing brute-force protection on the WebDAV endpoints via the basic auth header allowed to brute-force user credentials when the provided user name was not an email address. Users from version 24.0.0 onward are affected. This issue has been addressed in releases 24.0.11, 25.0.5 and 26.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Detail
CVE-2023-2942	Improper Input Validation in GitHub repository openemr/openemr prior to 7.0.1.	8.1	More Detail
CVE-2023-28382	Directory traversal vulnerability in ESS REC Agent Server Edition series allows an authenticated attacker to view or alter an arbitrary file on the server. Affected products and versions are as follows: ESS REC Agent Server Edition for Linux V1.0.0 to V1.4.3, ESS REC Agent Server Edition for Solaris V1.1.0 to V1.4.0, ESS REC Agent Server Edition for HP-UX V1.1.0 to V1.4.0, and ESS REC Agent Server Edition for AIX V1.2.0 to V1.4.1	8.1	More Detail
CVE-2023-31128	NextCloud Cookbook is a recipe library app. Prior to commit a46d9855 on the `master` branch and commit 489bb744 on the `main-0.9.x` branch, the `pull-checks.yml` workflow is vulnerable to command injection attacks because of using an untrusted `github.head_ref` field. The `github.head_ref` value is an attacker-controlled value. Assigning the value to `zzz";echo${IFS}"hello";#` can lead to command injection. Since the permission is not restricted, the attacker has a write-access to the repository. This issue is fixed in commit a46d9855 on the `master` branch and commit 489bb744 on the `main-0.9.x` branch. There is no risk for the user of the app within the NextCloud server. This only affects the main repository and possible forks of it. Those who have forked the NextCloud Cookbook repository should make sure their forks are on the latest version to prevent code injection attacks and similar.	8.1	More Detail
CVE-2023-2885	Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability in CBOT Chatbot allows Adversary in the Middle (AiTM).This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.	8.1	More Detail
CVE-2023-32074	user_oidc app is an OpenID Connect user backend for Nextcloud. Authentication can be broken/bypassed in user_oidc app. It is recommended that the Nextcloud user_oidc app is upgraded to 1.3.2	8.0	More Detail
CVE-2022-4815	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.1 and 9.3.0.3, including 8.3.x deserialize untrusted JSON data without constraining the parser to approved classes and methods.	8.0	More Detail
CVE-2023-31748	Insecure permissions in MobileTrans v4.0.11 allows attackers to escalate privileges to local admin via replacing the executable file.	7.8	More Detail
CVE-2023-30601	Privilege escalation when enabling FQL/Audit logs allows user with JMX access to run arbitrary commands as the user running Apache Cassandra This issue affects Apache Cassandra: from 4.0.0 through 4.0.9, from 4.1.0 through 4.1.1. WORKAROUND The vulnerability requires nodetool/JMX access to be exploitable, disable access for any non-trusted users. MITIGATION Upgrade to 4.0.10 or 4.1.2 and leave the new FQL/Auditlog configuration property allow_nodetool_archive_command as false.	7.8	More Detail
CVE-2021-25749	Windows workloads can run as ContainerAdministrator even when those workloads set the runAsNonRoot option to true.	7.8	More Detail
CVE-2023-0950	Improper Validation of Array Index vulnerability in the spreadsheet component of The Document Foundation LibreOffice allows an attacker to craft a spreadsheet document that will cause an array index underflow when loaded. In the affected versions of LibreOffice certain malformed spreadsheet formulas, such as AGGREGATE, could be created with less parameters passed to the formula interpreter than it expected, leading to an array index underflow, in which case there is a risk that arbitrary code could be executed. This issue affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.6; 7.5 versions prior to 7.5.1.	7.8	More Detail
CVE-2022-47029	An issue was found in Action Launcher v50.5 allows an attacker to escalate privilege via modification of the intent string to function update.	7.8	More Detail
CVE-2023-22970	Bottles before 51.0 mishandles YAML load, which allows remote code execution via a crafted file.	7.8	More Detail
CVE-2023-29738	An issue found in Wave Animated Keyboard Emoji v.1.70.7 for Android allows a local attacker to cause code execution and escalation of Privileges via the database files.	7.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-31873	Gin 0.7.4 allows execution of arbitrary code when a crafted file is opened, e.g., via require('child_process').	7.8	More Detail
CVE-2023-2939	Insufficient data validation in Installer in Google Chrome on Windows prior to 114.0.5735.90 allowed a local attacker to perform privilege escalation via crafted symbolic link. (Chromium security severity: Medium)	7.8	More Detail
CVE-2023-34153	A vulnerability was found in ImageMagick. This security flaw causes a shell command injection vulnerability via video:vsync or video:pixel-format options in VIDEO encoding/decoding.	7.8	More Detail
CVE-2023-26127	All versions of the package n158 are vulnerable to Command Injection due to improper input sanitization in the 'module.exports' function. **Note:** To execute the code snippet and potentially exploit the vulnerability, the attacker needs to have the ability to run Node.js code within the target environment. This typically requires some level of access to the system or application hosting the Node.js environment.	7.8	More Detail
CVE-2023-27529	Wacom Tablet Driver installer prior to 6.4.2-1 (for macOS) contains an improper link resolution before file access vulnerability. When a user is tricked to execute a small malicious script before executing the affected version of the installer, arbitrary code may be executed with the root privilege.	7.8	More Detail
CVE-2023-29733	The Lock Master app 2.2.4 for Android allows unauthorized apps to modify the values in its SharedPreference files. These files hold data that affects many app functions. Malicious modifications by unauthorized apps can cause security issues, such as functionality manipulation, resulting in a severe escalation of privilege attack.	7.8	More Detail
CVE-2023-32687	tgstation-server is a toolset to manage production BYOND servers. Starting in version 4.7.0 and prior to 5.12.1, instance users with the list chat bots permission can read chat bot connections strings without the associated permission. This issue is patched in version 5.12.1. As a workaround, remove the list chat bots permission from users that should not have the ability to view connection strings. Invalidate any credentials previously stored for safety.	7.7	More Detail
CVE-2023-26215	The server component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains a vulnerability that allows an attacker with low-privileged application access to read system files that are accessible to the web server. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.5.16 and below.	7.7	More Detail
CVE-2023-33248	Amazon Alexa software version 8960323972 on Echo Dot 2nd generation and 3rd generation devices potentially allows attackers to deliver security-relevant commands via an audio signal between 16 and 22 kHz (often outside the range of human adult hearing). Commands at these frequencies are essentially never spoken by authorized actors, but a substantial fraction of the commands are successful.	7.6	More Detail
CVE-2021-25748	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use a newline character to bypass the sanitization of the `spec.rules[].http.paths[].path` field of an Ingress object (in the `networking.k8s.io` or `extensions` API group) to obtain the credentials of the ingress-nginx controller. In the default configuration, that credential has access to all secrets in the cluster.	7.6	More Detail
CVE-2023-32307	Sofia-SIP is an open-source SIP User-Agent library, compliant with the IETF RFC3261 specification. Referring to [GHSA-8599-x7rq-fr54] (https://github.com/freeswitch/sofia-sip/security/advisories/GHSA-8599-x7rq-fr54), several other potential heap-over-flow and integer-overflow in stun_parse_attr_error_code and stun_parse_attr_uint32 were found because the lack of attributes length check when Sofia-SIP handles STUN packets. The previous patch of [GHSA-8599-x7rq-fr54](https://github.com/freeswitch/sofia-sip/security/advisories/GHSA-8599-x7rq-fr54) fixed the vulnerability when attr_type did not match the enum value, but there are also vulnerabilities in the handling of other valid cases. The OOB read and integer-overflow made by attacker may lead to crash, high consumption of memory or even other more serious consequences. These issue have been addressed in version 1.13.15. Users are advised to upgrade.	7.5	More Detail
CVE-2023-31594	IC Realtime ICIP-P2012T 2.420 is vulnerable to Incorrect Access Control via an exposed HTTP channel using VLC network.	7.5	More Detail
CVE-2023-2480	Missing access permissions checks in M-Files Client before 23.5.12598.0 (excluding 23.2 SR2 and newer) allows elevation of privilege via UI extension applications	7.5	More Detail
CVE-2023-21516	XSS vulnerability from InstantPlay in Galaxy Store prior to version 4.5.49.8 allows attackers to execute javascript API to install APK from Galaxy Store.	7.5	More Detail
CVE-2023-33974	RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. In versions 2023.01 and prior, an attacker can send multiple crafted frames to the device to trigger a race condition. The race condition invalidates assumptions about the program state and leads to an invalid memory access resulting in denial of service. This issue is patched in pull request 19679. There are no known workarounds.	7.5	More Detail
CVE-2023-31861	ZLMediaKit 4.0 is vulnerable to Directory Traversal.	7.5	More Detail
CVE-2023-21515	InstantPlay which included vulnerable script which could execute javascript in Galaxy Store prior to version 4.5.49.8 allows attackers to execute javascript API to install APK from Galaxy Store.	7.5	More Detail
CVE-2023-32067	c-ares is an asynchronous resolver library. c-ares is vulnerable to denial of service. If a target resolver sends a query, the attacker forges a malformed UDP packet with a length of 0 and returns them to the target resolver. The target resolver erroneously interprets the 0 length as a graceful shutdown of the connection. This issue has been patched in version 1.19.1.	7.5	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-33973	RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. In versions 2023.01 and prior, an attacker can send a crafted frame which is forwarded by the device. During encoding of the packet a NULL pointer dereference occurs. This crashes the device leading to denial of service. A patch is available at pull request 19678. There are no known workarounds.	7.5	More Detail
CVE-2023-21514	Improper scheme validation from InstantPlay Deeplink in Galaxy Store prior to version 4.5.49.8 allows attackers to execute javascript API to install APK from Galaxy Store.	7.5	More Detail
CVE-2023-2968	A remote attacker can trigger a denial of service in the socket.remoteAddress variable, by sending a crafted HTTP request. Usage of the undefined variable raises a TypeError exception.	7.5	More Detail
CVE-2023-31227	The hwPartsDFR module has a vulnerability in API calling verification. Successful exploitation of this vulnerability may affect device confidentiality.	7.5	More Detail
CVE-2023-29731	SoLive 1.6.14 thru 1.6.20 for Android has an exposed component that provides a method to modify the SharedPreference file. An attacker can leverage this method to inject a large amount of data into any SharedPreference file, which will be loaded into memory when the application is opened. When an attacker injects too much data, the application will trigger an OOM error and crash at startup, resulting in a persistent denial of service.	7.5	More Detail
CVE-2023-33263	In WFTPD 3.25, usernames and password hashes are stored in an openly viewable wftpd.ini configuration file within the WFTPD directory. NOTE: this is a product from 2006.	7.5	More Detail
CVE-2023-31185	ROZCOM server framework - Misconfiguration may allow information disclosure via an unspecified request.	7.5	More Detail
CVE-2023-33192	ntpd-rs is an NTP implementation written in Rust. ntpd-rs does not validate the length of NTS cookies in received NTP packets to the server. An attacker can crash the server by sending a specially crafted NTP packet containing a cookie shorter than what the server expects. The server also crashes when it is not configured to handle NTS packets. The issue was caused by improper slice indexing. The indexing operations were replaced by safer alternatives that do not crash the ntpd-rs server process but instead properly handle the error condition. A patch was released in version 0.3.3.	7.5	More Detail
CVE-2023-31226	The SDK for the MediaPlaybackController module has improper permission verification. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Detail
CVE-2023-28319	A use after free vulnerability exists in curl <v8.1.0 in the way libcurl offers a feature to verify an SSH server's public key using a SHA 256 hash. When this check fails, libcurl would free the memory for the fingerprint before it returns an error message containing the (now freed) hash. This flaw risks inserting sensitive heap-based data into the error message that might be shown to users or otherwise get leaked and revealed.	7.5	More Detail
CVE-2023-29380	Warpinator before 1.6.0 allows remote file deletion via directory traversal in top_dir_basenames.	7.5	More Detail
CVE-2023-29726	The Call Blocker application 6.6.3 for Android incorrectly opens a key component that an attacker can use to inject large amounts of dirty data into the application's database. When the application starts, it loads the data from the database into memory. Once the attacker injects too much data, the application triggers an OOM error and crashes, resulting in a persistent denial of service.	7.5	More Detail
CVE-2023-30570	pluto in Libreswan before 4.11 allows a denial of service (responder SPI mishandling and daemon crash) via unauthenticated IKEv1 Aggressive Mode packets. The earliest affected version is 3.28.	7.5	More Detail
CVE-2023-33740	Incorrect access control in luowice v3.5.18 allows attackers to access cloud source code information via modification fo the Verify parameter in a warning message.	7.5	More Detail
CVE-2023-33741	Macrovideo v380pro v1.4.97 shares the device id and password when sharing the device.	7.5	More Detail
CVE-2021-46883	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail
CVE-2021-46884	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail
CVE-2021-46885	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail
CVE-2021-46886	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-48480	Integer overflow vulnerability in some phones. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Detail
CVE-2021-27825	A directory traversal vulnerability on Mercury MAC1200R devices allows attackers to read arbitrary files via a web-static/ URL.	7.5	More Detail
CVE-2023-2953	A vulnerability was found in openldap. This security flaw causes a null pointer dereference in ber_memalloc_x() function.	7.5	More Detail
CVE-2023-0116	The reminder module lacks an authentication mechanism for broadcasts received. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail
CVE-2023-29740	An issue found in Alarm Clock for Heavy Sleepers v.5.3.2 for Android allows unauthorized apps to cause a denial of service attack by manipulating the database.	7.5	More Detail
CVE-2023-29743	An issue found in BestWeather v.7.3.1 for Android allows unauthorized apps to cause a persistent denial of service attack by manipulating the database.	7.5	More Detail
CVE-2023-20883	In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.	7.5	More Detail
CVE-2023-31763	Weak security in the transmitter of AGShome Smart Alarm v1.0 allows attackers to gain full access to the system via a code replay attack.	7.5	More Detail
CVE-2023-31762	Weak security in the transmitter of Digoo DG-HAMB Smart Home Security System v1.0 allows attackers to gain full access to the system via a code replay attack.	7.5	More Detail
CVE-2023-31761	Weak security in the transmitter of Blitzwolf BW-IS22 Smart Home Security Alarm v1.0 allows attackers to gain full access to the system via a code replay attack.	7.5	More Detail
CVE-2023-31759	Weak Security in the 433MHz keyfob of Kerui W18 Alarm System v1.0 allows attackers to gain full access via a code replay attack.	7.5	More Detail
CVE-2023-32342	IBM GSKit could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 255828.	7.5	More Detail
CVE-2023-2798	Those using HtmlUnit to browse untrusted webpages may be vulnerable to Denial of service attacks (DoS). If HtmlUnit is running on user supplied web pages, an attacker may supply content that causes HtmlUnit to crash by a stack overflow. This effect may support a denial of service attack.This issue affects htmlunit before 2.70.0.	7.5	More Detail
CVE-2021-46882	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail
CVE-2023-31595	IC Realtime ICIP-P2012T 2.420 is vulnerable to Incorrect Access Control via unauthenticated port access.	7.5	More Detail
CVE-2023-23755	An issue was discovered in Joomla! 4.2.0 through 4.3.1. The lack of rate limiting allowed brute force attacks against MFA methods.	7.5	More Detail
CVE-2021-46881	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	7.5	More Detail
CVE-2023-32763	An issue was discovered in Qt before 5.15.15, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. When a SVG file with an image inside it is rendered, a QTextLayout buffer overflow can be triggered.	7.5	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-33980	Bramble Synchronisation Protocol (BSP) in Briar before 1.4.22 allows attackers to cause a denial of service (repeated application crashes) via a series of long messages to a contact.	7.5	More Detail
CVE-2023-30196	Prestashop salesbooster <= 1.10.4 is vulnerable to Incorrect Access Control via modules/salesbooster/downloads/download.php.	7.5	More Detail
CVE-2023-33355	IceCMS v1.0.0 has Insecure Permissions. There is unauthorized access to the API, resulting in the disclosure of sensitive information.	7.5	More Detail
CVE-2023-33247	Talend Data Catalog remote harvesting server before 8.0-20230413 contains a /upgrade endpoint that allows an unauthenticated WAR file to be deployed on the server. (A mitigation is that the remote harvesting server should be behind a firewall that only allows access to the Talend Data Catalog server.)	7.5	More Detail
CVE-2023-26130	Versions of the package yhirose/cpp-httplib before 0.12.4 are vulnerable to CRLF Injection when untrusted user input is used to set the content-type header in the HTTP .Patch, .Post, .Put and .Delete requests. This can lead to logical errors and other misbehaviors. **Note:** This issue is present due to an incomplete fix for [CVE-2020-11709](https://security.snyk.io/vuln/SNYK-UNMANAGED-YHIROSECPPHTTPLIB-2366507).	7.5	More Detail
CVE-2023-24825	RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2023.04, an attacker can send a crafted frame to the device to trigger a NULL pointer dereference leading to denial of service. This issue is fixed in version 2023.04. There are no known workarounds.	7.5	More Detail
CVE-2023-24817	RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2023.04, an attacker can send a crafted frame to the device resulting in an integer underflow and out of bounds access in the packet buffer. Triggering the access at the right time will corrupt other packets or the allocator metadata. Corrupting a pointer will lead to denial of service. This issue is fixed in version 2023.04. As a workaround, disable SRH in the network stack.	7.5	More Detail
CVE-2023-25599	A vulnerability in the conferencing component of Mitel MiVoice Connect through 19.3 SP2, 22.24.1500.0 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient validation for the test_presenter.php page. A successful exploit could allow an attacker to execute arbitrary scripts.	7.4	More Detail
CVE-2023-33291	In ebankIT 6, the public endpoints /public/token/Email/generate and /public/token/SMS/generate allow generation of OTP messages to any e-mail address or phone number without validation. (It cannot be exploited with e-mail addresses or phone numbers that are registered in the application.)	7.4	More Detail
CVE-2023-33983	The Introduction Client in Briar through 1.5.3 does not implement out-of-band verification for the public keys of introducees. An introducer can launch man-in-the-middle attacks against later private communication between two introduced parties.	7.4	More Detail
CVE-2023-32695	socket.io parser is a socket.io encoder and decoder written in JavaScript complying with version 5 of socket.io-protocol. A specially crafted Socket.IO packet can trigger an uncaught exception on the Socket.IO server, thus killing the Node.js process. A patch has been released in version 4.2.3.	7.3	More Detail
CVE-2023-0329	The Elementor Website Builder WordPress plugin before 3.12.2 does not properly sanitize and escape the Replace URL parameter in the Tools module before using it in a SQL statement, leading to a SQL injection exploitable by users with the Administrator role.	7.2	More Detail
CVE-2022-24628	An issue was discovered in AudioCodes Device Manager Express through 7.8.20002.47752. It is authenticated SQL injection in the id parameter of IPPhoneFirmwareEdit.php.	7.2	More Detail
CVE-2023-32318	Nextcloud server provides a home for data. A regression in the session handling between Nextcloud Server and the Nextcloud Text app prevented a correct destruction of the session on logout if cookies were not cleared manually. After successfully authenticating with any other account the previous session would be continued and the attacker would be authenticated as the previously logged in user. It is recommended that the Nextcloud Server is upgraded to 25.0.6 or 26.0.1.	7.2	More Detail
CVE-2022-24630	An issue was discovered in AudioCodes Device Manager Express through 7.8.20002.47752. BrowseFiles.php allows a ?cmd=ssh POST request with an ssh_command field that is executed.	7.2	More Detail
CVE-2023-33439	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to SQL Injection via /eval/admin/manage_task.php?id=.	7.2	More Detail
CVE-2023-27988	The post-authentication command injection vulnerability in the Zyxel NAS326 firmware versions prior to V5.21(AAZF.13)C0 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device remotely.	7.2	More Detail
CVE-2023-33440	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to arbitrary code execution via /eval/ajax.php?action=save_user.	7.2	More Detail
CVE-2023-33234	Arbitrary code execution in Apache Airflow CNCF Kubernetes provider version 5.0.0 allows user to change xcom sidecar image and resources via Airflow connection. In order to exploit this weakness, a user would already need elevated permissions (Op or Admin) to change the connection object in this manner. Operators should upgrade to provider version 7.0.0 which has removed the vulnerability.	7.2	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-31460	A vulnerability in the Connect Mobility Router component of MiVoice Connect versions 9.6.2208.101 and earlier could allow an authenticated attacker with internal network access to conduct a command injection attack due to insufficient restriction on URL parameters.	7.2	More Detail
CVE-2023-29098	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ArtistScope CopySafe Web Protection plugin <= 3.13 versions.	7.1	More Detail
CVE-2023-27613	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in MonitorClick Forms Ada – Form Builder plugin <= 1.0 versions.	7.1	More Detail
CVE-2023-33326	Unauth. Reflected (XSS) Cross-Site Scripting (XSS) vulnerability in EventPrime plugin <= 2.8.6 versions.	7.1	More Detail
CVE-2023-2496	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to unauthorized arbitrary file uploads due to an improper capability check on the 'validate_upload' function in versions up to, and including, 3.3.19. This makes it possible for authenticated attackers with a role that the administrator previously granted access to the plugin to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.1	More Detail
CVE-2023-32698	nFPM is an alternative to fpm. The file permissions on the checked-in files were not maintained. Hence, when nfpm packaged the files (without extra config for enforcing it's own permissions) files could go out with bad permissions (chmod 666 or 777). Anyone using nfpm for creating packages without checking/setting file permissions before packaging could result in bad permissions for files/folders.	7.1	More Detail
CVE-2023-33926	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Easy Google Maps plugin <= 1.11.7 versions.	7.1	More Detail
CVE-2023-33319	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce WooCommerce Follow-Up Emails (AutomateWoo) plugin <= 4.9.40 versions.	7.1	More Detail
CVE-2022-41221	The client in OpenText Archive Center Administration through 21.2 allows XXE attacks. Authenticated users of the OpenText Archive Center Administration client (Versions 16.2.3, 21.2, and older versions) could upload XML files to the application that it did not sufficiently validate. As a result, attackers could craft XML files that, when processed by the application, would cause a negative security impact such as data exfiltration or localized denial of service against the application instance and system of the user running it.	7.1	More Detail
CVE-2023-32800	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in One Rank Math SEO PRO plugin <= 3.0.35 versions.	7.1	More Detail
CVE-2023-33309	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Awesome Motive Duplicator Pro plugin <= 4.5.11 versions.	7.1	More Detail
CVE-2022-39071	There is an unauthorized access vulnerability in some ZTE mobile phones. If a malicious application is installed on the phone, it could overwrite some system configuration files and user installers without user permission.	7.1	More Detail
CVE-2022-39075	There is an unauthorized access vulnerability in some ZTE mobile phones. If a malicious application is installed on the phone, it could delete some system files without user permission.	7.1	More Detail
CVE-2023-33332	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Product Vendors plugin <= 2.1.76 versions.	7.1	More Detail
CVE-2023-32316	CloudExplorer Lite is an open source cloud management tool. In affected versions users can add themselves to any organization in CloudExplorer Lite. This is due to a missing permission check on the user profile. It is recommended to upgrade the version to v1.1.0. There are no known workarounds for this vulnerability.	7.1	More Detail
CVE-2022-45366	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Jason Crouse, VeronaLabs Slimstat Analytics plugin <= 5.0.4 versions.	7.1	More Detail
CVE-2023-32311	CloudExplorer Lite is an open source cloud management platform. In CloudExplorer Lite prior to version 1.1.0 users organization/workspace permissions are not properly checked. This allows users to add themselves to any organization. This vulnerability has been fixed in v1.1.0. Users are advised to upgrade. There are no known workarounds for this issue.	7.1	More Detail
CVE-2023-28079	PowerPath for Windows, versions 7.0, 7.1 & 7.2 contains Insecure File and Folder Permissions vulnerability. A regular user (non-admin) can exploit the weak folder and file permissions to escalate privileges and execute arbitrary code in the context of NT AUTHORITY\SYSTEM.	7.0	More Detail
CVE-2022-46361	An attacker having physical access to WDM can plug USB device to gain access and execute unwanted commands. A malicious user could enter a system command along with a backup configuration, which could result in the execution of unwanted commands. This issue affects OneWireless all versions up to 322.1 and fixed in version 322.2.	6.9	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-2002	A vulnerability was found in the HCI sockets implementation due to a missing capability check in net/bluetooth/hci_sock.c in the Linux Kernel. This flaw allows an attacker to unauthorized execution of management commands, compromising the confidentiality, integrity, and availability of Bluetooth communication.	6.8	More Detail
CVE-2023-28080	PowerPath for Windows, versions 7.0, 7.1 & 7.2 contains DLL Hijacking Vulnerabilities. A regular user (non-admin) can exploit these issues to potentially escalate privileges and execute arbitrary code in the context of NT AUTHORITY\SYSTEM.	6.7	More Detail
CVE-2022-0357	Unquoted Search Path or Element vulnerability in the Vulnerability Scan component of Bitdefender Total Security, Bitdefender Internet Security, and Bitdefender Antivirus Plus allows an attacker to elevate privileges to SYSTEM. This issue affects: Bitdefender Total Security versions prior to 26.0.10.45. Bitdefender Internet Security versions prior to 26.0.10.45. Bitdefender Antivirus Plus versions prior to 26.0.10.45.	6.7	More Detail
CVE-2023-0779	At the most basic level, an invalid pointer can be input that crashes the device, but with more knowledge of the device's memory layout, further exploitation is possible.	6.7	More Detail
CVE-2023-32676	Autolab is a course management service that enables auto-graded programming assignments. A Tar slip vulnerability was found in the Install assessment functionality of Autolab. To exploit this vulnerability an authenticated attacker with instructor permissions needs to upload a specially crafted Tar file. Using the install assessment functionality an attacker can feed a Tar file that contain files with paths pointing outside of the target directory (e.g., `../../../../tmp/tarslipped1.sh`). When the Install assessment form is submitted the files inside of the archives are expanded to the attacker-chosen locations. This issue has been addressed in version 2.11.0. Users are advised to upgrade.	6.7	More Detail
CVE-2023-32317	Autolab is a course management service that enables auto-graded programming assignments. A Tar slip vulnerability was found in the MOSS cheat checker functionality of Autolab. To exploit this vulnerability an authenticated attacker with instructor permissions needs to upload a specially crafted Tar file. Both "Base File Tar" and "Additional file archive" can be fed with Tar files that contain paths outside their target directories (e.g., `../../../../tmp/tarslipped2.sh`). When the MOSS cheat checker is started the files inside of the archives are expanded to the attacker-chosen locations. This issue may lead to arbitrary file write within the scope of the running process. This issue has been addressed in version 2.11.0. Users are advised to upgrade.	6.7	More Detail
CVE-2022-45853	The privilege escalation vulnerability in the Zyxel GS1900-8 firmware version V2.70(AAHH.3) and the GS1900-8HP firmware version V2.70(AAHI.3) could allow an authenticated, local attacker with administrator privileges to execute some system commands as 'root' on a vulnerable device via SSH.	6.7	More Detail
CVE-2023-34204	imapsync through 2.229 uses predictable paths under /tmp and /var/tmp in its default mode of operation. Both of these are typically world-writable, and thus (for example) an attacker can modify imapsync's cache and overwrite files belonging to the user who runs it.	6.5	More Detail
CVE-2023-2283	A vulnerability was found in libssh, where the authentication check of the connecting client can be bypassed in the`pki_verify_data_signature` function in memory allocation problems. This issue may happen if there is insufficient memory or the memory usage is limited. The problem is caused by the return value `rc,` which is initialized to SSH_ERROR and later rewritten to save the return value of the function call `pki_key_check_hash_compatible.` The value of the variable is not changed between this point and the cryptographic verification. Therefore any error between them calls `goto error` returning SSH_OK.	6.5	More Detail
CVE-2023-2940	Inappropriate implementation in Downloads in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Detail
CVE-2023-33981	Briar before 1.4.22 allows attackers to spoof other users' messages in a blog, forum, or private group, but each spoofed message would need to be an exact duplicate of a legitimate message displayed alongside the spoofed one.	6.5	More Detail
CVE-2023-33720	mp4v2 v2.1.2 was discovered to contain a memory leak via the class MP4BytesProperty.	6.5	More Detail
CVE-2023-33950	Pattern Redirects in Liferay Portal 7.4.3.48 through 7.4.3.76, and Liferay DXP 7.4 update 48 through 76 allows regular expressions that are vulnerable to ReDoS attacks to be used as patterns, which allows remote attackers to consume an excessive amount of server resources via crafted request URLs.	6.5	More Detail
CVE-2023-24603	OX App Suite before backend 7.10.6-rev37 does not check size limits when downloading, e.g., potentially allowing a crafted iCal feed to provide an unlimited amount of data.	6.5	More Detail
CVE-2023-1667	A NULL pointer dereference was found In libssh during re-keying with algorithm guessing. This issue may allow an authenticated client to cause a denial of service.	6.5	More Detail
CVE-2023-1664	A flaw was found in Keycloak. This flaw depends on a non-default configuration "Revalidate Client Certificate" to be enabled and the reverse proxy is not validating the certificate before Keycloak. Using this method an attacker may choose the certificate which will be validated by the server. If this happens and the KC_SPI_TRUSTSTORE_FILE_FILE variable is missing/misconfigured, any trustfile may be accepted with the logging information of "Cannot validate client certificate trust: Truststore not available". This may not impact availability as the attacker would have no access to the server, but consumer applications Integrity or Confidentiality may be impacted considering a possible access to them. Considering the environment is correctly set to use "Revalidate Client Certificate" this flaw is avoidable.	6.5	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-2650	Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(n^2) with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low.	6.5	More Detail
CVE-2023-33311	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in CRM Perks Contact Form Entries plugin <= 1.3.0 versions.	6.5	More Detail
CVE-2023-22504	Affected versions of Atlassian Confluence Server allow remote attackers who have read permissions to a page, but not write permissions, to upload attachments via a Broken Access Control vulnerability in the attachments feature.	6.5	More Detail
CVE-2023-28785	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Yoast Yoast SEO: Local plugin <= 14.9 versions.	6.5	More Detail
CVE-2023-33180	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered starting in version 3.2.0 and prior to version 3.3.2 in the `/display/map` API route inside the CMS. This allows an authenticated user to exfiltrate data from the Xibo database by injecting specially crafted values in to the `bounds` parameter. Users should upgrade to version 3.3.5, which fixes this issue. There are no known workarounds aside from upgrading.	6.5	More Detail
CVE-2023-32699	MeterSphere is an open source continuous testing platform. Version 2.9.1 and prior are vulnerable to denial of service. The `checkUserPassword` method is used to check whether the password provided by the user matches the password saved in the database, and the `CodingUtil.md5` method is used to encrypt the original password with MD5 to ensure that the password will not be saved in plain text when it is stored. If a user submits a very long password when logging in, the system will be forced to execute the long password MD5 encryption process, causing the server CPU and memory to be exhausted, thereby causing a denial of service attack on the server. This issue is fixed in version 2.10.0-lts with a maximum password length.	6.5	More Detail
CVE-2023-1524	The Download Manager WordPress plugin before 3.2.71 does not adequately validate passwords for password-protected files. Upon validation, a master key is generated and exposed to the user, which may be used to download any password-protected file on the server, allowing a user to download any file with the knowledge of any one file's password.	6.5	More Detail
CVE-2023-31187	Avaya IX Workforce Engagement v15.2.7.1195 - CWE-522: Insufficiently Protected Credentials	6.5	More Detail
CVE-2023-2804	A heap-based buffer overflow issue was discovered in libjpeg-turbo in h2v2_merged_upsample_internal() function of jdmrgext.c file. The vulnerability can only be exploited with 12-bit data precision for which the range of the sample data type exceeds the valid sample range, hence, an attacker could craft a 12-bit lossless JPEG image that contains out-of-range 12-bit samples. An application attempting to decompress such image using merged upsampling would lead to segmentation fault or buffer overflows, causing an application to crash.	6.5	More Detail
CVE-2022-39374	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. If Synapse and a malicious homeserver are both joined to the same room, the malicious homeserver can trick Synapse into accepting previously rejected events into its view of the current state of that room. This can be exploited in a way that causes all further messages and state changes sent in that room from the vulnerable homeserver to be rejected. This issue has been patched in version 1.68.0	6.5	More Detail
CVE-2023-33179	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered starting in version 3.2.0 and prior to version 3.3.5 in the `nameFilter` function used throughout the CMS. This allows an authenticated user to exfiltrate data from the Xibo database by injecting specially crafted values for logical operators. Users should upgrade to version 3.3.5 which fixes this issue. There are no known workarounds aside from upgrading.	6.5	More Detail
CVE-2023-33178	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the `/dataset/data/{id}` API route inside the CMS starting in version 1.4.0 and prior to versions 2.3.17 and 3.3.5. This allows an authenticated user to exfiltrate data from the Xibo database by injecting specially crafted values in to the `filter` parameter. Values allowed in the filter parameter are checked against a deny list of commands that should not be allowed, however this checking was done in a case sensitive manor and so it is possible to bypass these checks by using unusual case combinations. Users should upgrade to version 2.3.17 or 3.3.5, which fix this issue. There are no workarounds aside from upgrading.	6.5	More Detail
CVE-2022-30025	SQL injection in "/Framewrk/Home.jsp" file (POST method) in tCredence Analytics iDEAL Wealth and Funds - 1.0 iallows authenticated remote attackers to inject payload via "v" parameter.	6.5	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-23699	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Chris Reynolds Progress Bar plugin <= 2.2.1 versions.	6.5	More Detail
CVE-2022-4240	Missing Authentication for Critical Function vulnerability in Honeywell OneWireless allows Authentication Bypass. This issue affects OneWireless version 322.1	6.5	More Detail
CVE-2023-0459	Copy_from_user on 64-bit versions of the Linux kernel does not implement the __uaccess_begin_nospec allowing a user to bypass the "access_ok" check and pass a kernel pointer to copy_from_user(). This would allow an attacker to leak information. We recommend upgrading beyond commit 74e19ef0ff8061ef55957c3abd71614ef0f42f47	6.5	More Detail
CVE-2023-33945	SQL injection vulnerability in the upgrade process for SQL Server in Liferay Portal 7.3.1 through 7.4.3.17, and Liferay DXP 7.3 before update 6, and 7.4 before update 18 allows attackers to execute arbitrary SQL commands via the name of a database table's primary key index. This vulnerability is only exploitable when chained with other attacks. To exploit this vulnerability, the attacker must modify the database and wait for the application to be upgraded.	6.4	More Detail
CVE-2023-2498	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.3.19 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Detail
CVE-2023-28153	An issue was discovered in the Kiddoware Kids Place Parental Control application before 3.8.50 for Android. The child can remove all restrictions temporarily without the parents noticing by rebooting into Android Safe Mode and disabling the "Display over other apps" permission.	6.4	More Detail
CVE-2023-2928	A vulnerability was found in DedeCMS up to 5.7.106. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file uploads/dede/article_allowurl_edit.php. The manipulation of the argument allurls leads to code injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-230083.	6.3	More Detail
CVE-2023-2951	A vulnerability classified as critical has been found in code-projects Bus Dispatch and Information System 1.0. Affected is an unknown function of the file delete_bus.php. The manipulation of the argument busid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230112.	6.3	More Detail
CVE-2023-2927	A vulnerability was found in JIZHICMS 2.4.5. It has been classified as critical. Affected is the function index of the file TemplateController.php. The manipulation of the argument webapi leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-230082 is the identifier assigned to this vulnerability.	6.3	More Detail
CVE-2023-2879	GDSDB infinite loop in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via packet injection or crafted capture file	6.3	More Detail
CVE-2014-125101	A vulnerability classified as critical has been found in Portfolio Gallery Plugin up to 1.1.8 on WordPress. This affects an unknown part. The manipulation leads to sql injection. It is possible to initiate the attack remotely. Upgrading to version 1.1.9 is able to address this issue. The identifier of the patch is 58ed88243e17df766036f4857041edaf358076d3. It is recommended to upgrade the affected component. The identifier VDB-230085 was assigned to this vulnerability.	6.3	More Detail
CVE-2023-2955	A vulnerability, which was classified as critical, was found in SourceCodester Students Online Internship Timesheet System 1.0. Affected is an unknown function of the file rendered_report.php of the component GET Parameter Handler. The manipulation of the argument sid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-230142 is the identifier assigned to this vulnerability.	6.3	More Detail
CVE-2023-2923	A vulnerability classified as critical was found in Tenda AC6 US_AC6V1.0BR_V15.03.05.19. Affected by this vulnerability is the function fromDhcpListClient. The manipulation leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-230077 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Detail
CVE-2023-33188	Omni-notes is an open source note-taking application for Android. The Omni-notes Android app had an insufficient path validation vulnerability when displaying the details of a note received through an externally-provided intent. The paths of the note's attachments were not properly validated, allowing malicious or compromised applications in the same device to force Omni-notes to copy files from its internal storage to its external storage directory, where they would have become accessible to any component with permission to read the external storage. Updating to the newest version (6.2.7) of Omni-notes Android fixes this vulnerability.	6.3	More Detail
CVE-2015-10106	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in mback2k mh_httpbl Extension up to 1.1.7 on TYPO3. This vulnerability affects the function moduleContent of the file mod1/index.php. The manipulation leads to sql injection. The attack can be initiated remotely. Upgrading to version 1.1.8 is able to address this issue. The patch is identified as 429f50f4e4795b20dae06735b41fb94f010722bf. It is recommended to upgrade the affected component. VDB-230086 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Detail
CVE-2023-2865	A vulnerability was found in SourceCodester Theme Park Ticketing System 1.0. It has been classified as critical. This affects an unknown part of the file print_ticket.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229821 was assigned to this vulnerability.	6.3	More Detail
CVE-2023-2980	A vulnerability classified as critical was found in Abstrium Pydio Cells 4.2.0. This vulnerability affects unknown code of the component User Creation Handler. The manipulation leads to improper control of resource identifiers. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.2.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-230212.	6.3	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-32689	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 5.4.4 and 6.1.1 are vulnerable to a phishing attack vulnerability that involves a user uploading malicious files. A malicious user could upload an HTML file to Parse Server via its public API. That HTML file would then be accessible at the internet domain at which Parse Server is hosted. The URL of the the uploaded HTML could be shared for phishing attacks. The HTML page may seem legitimate because it is served under the internet domain where Parse Server is hosted, which may be the same as a company's official website domain. An additional security issue arises when the Parse JavaScript SDK is used. The SDK stores sessions in the internet browser's local storage, which usually restricts data access depending on the internet domain. A malicious HTML file could contain a script that retrieves the user's session token from local storage and then share it with the attacker. The fix included in versions 5.4.4 and 6.1.1 adds a new Parse Server option `fileUpload.fileExtensions` to restrict file upload on Parse Server by file extension. It is recommended to restrict file upload for HTML file extensions, which this fix disables by default. If an app requires upload of files with HTML file extensions, the option can be set to `['.*']` or another custom value to override the default.	6.3	More Detail
CVE-2022-41987	Cross-Site Request Forgery (CSRF) vulnerability in LearningTimes BadgeOS plugin <= 3.7.1.6 versions.	6.3	More Detail
CVE-2023-30615	Iris is a web collaborative platform aiming to help incident responders sharing technical details during investigations. A stored Cross-Site Scripting (XSS) vulnerability has been identified in iris-web, affecting multiple locations . The vulnerability in allows an attacker to inject malicious scripts into the application, which are then executed when a user visits the affected locations. This can lead to unauthorized access, data theft, or other malicious activities. An attacker need to be authenticated on the application to exploit this vulnerability. The issue was patched in version 2.2.1 of iris-web.	6.3	More Detail
CVE-2023-31184	ROZCOM client CWE-798: Use of Hard-coded Credentials	6.2	More Detail
CVE-2022-43485	Use of Insufficiently Random Values in Honeywell OneWireless. This vulnerability may allow attacker to manipulate claims in client's JWT token. This issue affects OneWireless version 322.1	6.2	More Detail
CVE-2022-46907	A carefully crafted request on several JSPWiki plugins could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.12.0 or later.	6.1	More Detail
CVE-2023-2256	The Product Addons & Fields for WooCommerce WordPress plugin before 32.0.7 does not sanitize and escape some URL parameters, leading to Reflected Cross-Site Scripting.	6.1	More Detail
CVE-2023-2296	The Loginizer WordPress plugin before 1.7.9 does not escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Detail
CVE-2023-33198	tgstation-server is a production scale tool for BYOND server management. The DreamMaker API (DMAPI) chat channel cache can possibly be poisoned by a tgstation-server (TGS) restart and reattach. This can result in sending chat messages to one of any of the configured IRC or Discord channels for the instance on enabled chat bots. This lasts until the instance's chat channels are updated in TGS or DreamDaemon is restarted. TGS chat commands are unaffected, custom or otherwise.	6.1	More Detail
CVE-2023-2949	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.1.	6.1	More Detail
CVE-2023-25439	Stored Cross Site Scripting (XSS) vulnerability in Square Pig FusionInvoice 2023-1.0, allows attackers to execute arbitrary code via the description or content fields to the expenses, tasks, and customer details.	6.1	More Detail
CVE-2023-2023	The Custom 404 Pro WordPress plugin before 3.7.3 does not escape some URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting.	6.1	More Detail
CVE-2023-2948	Cross-site Scripting (XSS) - Generic in GitHub repository openemr/openemr prior to 7.0.1.	6.1	More Detail
CVE-2023-32218	Avaya IX Workforce Engagement v15.2.7.1195 - CWE-601: URL Redirection to Untrusted Site ('Open Redirect')	6.1	More Detail
CVE-2023-28370	Open redirect vulnerability in Tornado versions 6.3.1 and earlier allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having user access a specially crafted URL.	6.1	More Detail
CVE-2023-2518	The Easy Forms for Mailchimp WordPress plugin before 6.8.9 does not sanitise and escape a parameter before outputting it back in the page when the debug option is enabled, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Detail
CVE-2023-0733	The Newsletter Popup WordPress plugin through 1.2 does not sanitise and escape some of its settings, which could allow unauthenticated users to perform Stored Cross-Site Scripting attacks	6.1	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-20884	VMware Workspace ONE Access and VMware Identity Manager contain an insecure redirect vulnerability. An unauthenticated malicious actor may be able to redirect a victim to an attacker controlled domain due to improper path handling leading to sensitive information disclosure.	6.1	More Detail
CVE-2023-23754	An issue was discovered in Joomla! 4.2.0 through 4.3.1. Lack of input validation caused an open redirect and XSS issue within the new mfa selection screen.	6.1	More Detail
CVE-2023-20868	NSX-T contains a reflected cross-site scripting vulnerability due to a lack of input validation. A remote attacker can inject HTML or JavaScript to redirect to malicious pages.	6.1	More Detail
CVE-2023-24602	OX App Suite before frontend 7.10.6-rev24 allows XSS via data to the Tumblr portal widget, such as a post title.	6.1	More Detail
CVE-2023-33255	An issue was discovered in Papaya Viewer 1.0.1449. User-supplied input in form of DICOM or NIFTI images can be loaded into the Papaya web application without any kind of sanitization. This allows injection of arbitrary JavaScript code into image metadata, which is executed when that metadata is displayed in the Papaya web application.	6.1	More Detail
CVE-2023-24601	OX App Suite before frontend 7.10.6-rev24 allows XSS via a non-app deeplink such as the jslob API's registry sub-tree.	6.1	More Detail
CVE-2023-25598	A vulnerability in the conferencing component of Mitel MiVoice Connect through 19.3 SP2 and 20.x, 21.x, and 22.x through 22.24.1500.0 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient validation for the home.php page. A successful exploit could allow an attacker to execute arbitrary scripts.	6.1	More Detail
CVE-2023-33941	Multiple cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect class in Liferay Portal 7.4.3.41 through 7.4.3.52, and Liferay DXP 7.4 update 41 through 52 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter.	6.1	More Detail
CVE-2023-32681	Requests is a HTTP library. Since Requests 2.3.0, Requests has been leaking Proxy-Authorization headers to destination servers when redirected to an HTTPS endpoint. This is a product of how we use `rebuild_proxies` to reattach the `Proxy-Authorization` header to requests. For HTTP connections sent through the tunnel, the proxy will identify the header in the request itself and remove it prior to forwarding to the destination server. However when sent over HTTPS, the `Proxy-Authorization` header must be sent in the CONNECT request as the proxy has no visibility into the tunneled request. This results in Requests forwarding proxy credentials to the destination server unintentionally, allowing a malicious actor to potentially exfiltrate sensitive information. This issue has been patched in version 2.31.0.	6.1	More Detail
CVE-2023-33328	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PluginOps MailChimp Subscribe Form plugin <= 4.0.9.1 versions.	5.9	More Detail
CVE-2020-29547	An issue was discovered in Citadel through webcit-926. Meddler-in-the-middle attackers can pipeline commands after POP3 STLS, IMAP STARTTLS, or SMTP STARTTLS commands, injecting cleartext commands into an encrypted user session. This can lead to credential disclosure.	5.9	More Detail
CVE-2023-25028	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in chuyencode CC Custom Taxonomy plugin <= 1.0.1 versions.	5.9	More Detail
CVE-2023-33216	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gVectors Team WooDiscuz – WooCommerce Comments woodiscuz-woocommerce-comments allows Stored XSS.This issue affects WooDiscuz – WooCommerce Comments: from n/a through 2.2.9.	5.9	More Detail
CVE-2023-32958	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nose Graze Novelist plugin <= 1.2.0 versions.	5.9	More Detail
CVE-2023-32691	gost (GO Simple Tunnel) is a simple tunnel written in golang. Sensitive secrets such as passwords, token and API keys should be compared only using a constant-time comparison function. Untrusted input, sourced from a HTTP header, is compared directly with a secret. Since this comparison is not secure, an attacker can mount a side-channel timing attack to guess the password. As a workaround, this can be easily fixed using a constant time comparing function such as `crypto/subtle`'s `ConstantTimeCompare`.	5.9	More Detail
CVE-2023-33982	Bramble Handshake Protocol (BHP) in Briar before 1.5.3 is not forward secure: eavesdroppers can decrypt network traffic between two accounts if they later compromise both accounts. NOTE: the eavesdropping is typically impractical because BHP runs over an encrypted session that uses the Tor hidden service protocol.	5.9	More Detail
CVE-2023-33211	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in André Bräkling WP-Matomo Integration (WP-Piwik) plugin <= 1.0.27 versions.	5.9	More Detail
CVE-2023-25781	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sebastian Krysmanski Upload File Type Settings plugin <= 1.1 versions.	5.9	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-31147	c-ares is an asynchronous resolver library. When /dev/urandom or RtlGenRandom() are unavailable, c-ares uses rand() to generate random numbers used for DNS query ids. This is not a CSPRNG, and it is also not seeded by srand() so will generate predictable output. Input from the random number generator is fed into a non-compilant RC4 implementation and may not be as strong as the original RC4 implementation. No attempt is made to look for modern OS-provided CSPRNGs like arc4random() that is widely available. This issue has been fixed in version 1.19.1.	5.9	More Detail
CVE-2023-28321	An improper certificate validation vulnerability exists in curl <v8.1.0 in the way it supports matching of wildcard patterns when listed as "Subject Alternative Name" in TLS server certificates. curl can be built to use its own name matching function for TLS rather than one provided by a TLS library. This private wildcard matching function would match IDN (International Domain Name) hosts incorrectly and could as a result accept patterns that otherwise should mismatch. IDN hostnames are converted to puny code before used for certificate checks. Puny coded names always start with `xn--` and should not be allowed to pattern match, but the wildcard check in curl could still check for `x*`, which would match even though the IDN name most likely contained nothing even resembling an `x`.	5.9	More Detail
CVE-2023-24826	RIOT-OS, an operating system for Internet of Things (IoT) devices, contains a network stack with the ability to process 6LoWPAN frames. Prior to version 2023.04, an attacker can send crafted frames to the device to trigger the usage of an uninitialized object leading to denial of service. This issue is fixed in version 2023.04. As a workaround, disable fragment forwarding or SFR.	5.9	More Detail
CVE-2023-28320	A denial of service vulnerability exists in curl <v8.1.0 in the way libcurl provides several different backends for resolving host names, selected at build time. If it is built to use the synchronous resolver, it allows name resolves to time-out slow operations using `alarm()` and `siglongjmp()`. When doing this, libcurl used a global buffer that was not mutex protected and a multi-threaded application might therefore crash or otherwise misbehave.	5.9	More Detail
CVE-2023-20882	In Cloud foundry routing release versions from 0.262.0 and prior to 0.266.0,a bug in the gorouter process can lead to a denial of service of applications hosted on Cloud Foundry. Under the right circumstances, when client connections are closed prematurely, gorouter marks the currently selected backend as failed and removes it from the routing pool.	5.9	More Detail
CVE-2023-2875	A vulnerability, which was classified as problematic, was found in eScan Antivirus 22.0.1400.2443. Affected is the function 0x22E008u in the library PROCOBSRVESX.SYS of the component IoControlCode Handler. The manipulation leads to null pointer dereference. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-229854 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 Detail
CVE-2023-2872	A vulnerability classified as problematic has been found in FlexiHub 5.5.14691.0. This affects the function 0x220088 in the library fusbhub.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229851. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Detail
CVE-2022-47028	An issue discovered in Action Launcher for Android v50.5 allows an attacker to cause a denial of service via arbitary data injection to function insert.	5.5	More Detail
CVE-2023-29737	An issue found in Wave Animated Keyboard Emoji v.1.70.7 for Android allows a local attacker to cause a denial of service via the database files.	5.5	More Detail
CVE-2023-32448	PowerPath for Windows, versions 7.0, 7.1 & 7.2 contains License Key Stored in Cleartext vulnerability. A local user with access to the installation directory can retrieve the license key of the product and use it to install and license PowerPath on different systems.	5.5	More Detail
CVE-2023-33656	A memory leak vulnerability exists in NanoMQ 0.17.2. The vulnerability is located in the file message.c. An attacker could exploit this vulnerability to cause a denial of service attack by causing the program to consume all available memory resources.	5.5	More Detail
CVE-2023-33197	Craft is a CMS for creating custom digital experiences on the web. Cross-site scripting (XSS) can be triggered via the Update Asset Index utility. This issue has been patched in version 4.4.6.	5.5	More Detail
CVE-2023-29735	An issue found in edjing Mix v.7.09.01 for Android allows a local attacker to cause a denial of service via the database files.	5.5	More Detail
CVE-2023-33196	Craft is a CMS for creating custom digital experiences. Cross site scripting (XSS) can be triggered by review volumes. This issue has been fixed in version 4.4.7.	5.5	More Detail
CVE-2023-1981	A vulnerability was found in the avahi library. This flaw allows an unprivileged user to make a dbus call, causing the avahi daemon to crash.	5.5	More Detail
CVE-2023-2874	A vulnerability, which was classified as problematic, has been found in Twister Antivirus 8. This issue affects the function 0x804f2158/0x804f2154/0x804f2150/0x804f215c/0x804f2160/0x80800040/0x804f214c/0x804f2148/0x804f2144/0x801120e4/0x804f213c/0x804f2140 in the library filppd.sys of the component IoControlCode Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-229853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Detail
CVE-2023-23561	Stormshield Endpoint Security 2.3.0 through 2.3.2 has Incorrect Access Control: authenticated users can read sensitive information.	5.5	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-34151	A vulnerability was found in ImageMagick. This security flaw ouccers as an undefined behaviors of casting double to size_t in svg, mvg and other coders (recurring bugs of CVE-2022-32546).	5.5	More Detail
CVE-2021-4336	A vulnerability was found in ITRS Group monitor-ninja up to 2021.11.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file modules/reports/models/scheduled_reports.php. The manipulation leads to sql injection. Upgrading to version 2021.11.30 is able to address this issue. The name of the patch is 6da9080faec9bca1ca5342386c0421dca0a6c0cc. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-230084.	5.5	More Detail
CVE-2023-33789	A stored cross-site scripting (XSS) vulnerability in the Create Contact Groups (/tenancy/contact-groups/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33316	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Follow-Up Emails (AutomateWoo) plugin <= 4.9.40 versions.	5.4	More Detail
CVE-2022-42225	Jumpserver 2.10.0 <= version <= 2.26.0 contains multiple stored XSS vulnerabilities because of improper filtering of user input, which can execute any javascript under admin's permission.	5.4	More Detail
CVE-2023-33785	A stored cross-site scripting (XSS) vulnerability in the Create Rack Roles (/dcim/rack-roles/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33787	A stored cross-site scripting (XSS) vulnerability in the Create Tenant Groups (/tenancy/tenant-groups/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33788	A stored cross-site scripting (XSS) vulnerability in the Create Providers (/circuits/providers/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33786	A stored cross-site scripting (XSS) vulnerability in the Create Circuit Types (/circuits/circuit-types/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2022-46856	Cross-Site Request Forgery (CSRF) vulnerability in ORION Woocommerce Products Designer plugin <= 4.3.3 versions.	5.4	More Detail
CVE-2022-47448	Cross-Site Request Forgery (CSRF) vulnerability in dev.Xiligroup.Com - MS plugin <= 1.12.03 versions.	5.4	More Detail
CVE-2023-33790	A stored cross-site scripting (XSS) vulnerability in the Create Locations (/dcim/locations/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33962	JStachio is a type-safe Java Mustache templating engine. Prior to version 1.0.1, JStachio fails to escape single quotes `'` in HTML, allowing an attacker to inject malicious code. This vulnerability can be exploited by an attacker to execute arbitrary JavaScript code in the context of other users visiting pages that use this template engine. This can lead to various consequences, including session hijacking, defacement of web pages, theft of sensitive information, or even the propagation of malware. Version 1.0.1 contains a patch for this issue. To mitigate this vulnerability, the template engine should properly escape special characters, including single quotes. Common practice is to escape `'` as `&#39`. As a workaround, users can avoid this issue by using only double quotes `"` for HTML attributes.	5.4	More Detail
CVE-2022-33974	Cross-Site Request Forgery (CSRF) vulnerability in Smash Balloon Custom Twitter Feeds (Tweets Widget) plugin <= 1.8.4 versions.	5.4	More Detail
CVE-2022-47152	Cross-Site Request Forgery (CSRF) vulnerability in Etison, LLC ClickFunnels plugin <= 3.1.1 versions.	5.4	More Detail
CVE-2022-45364	Cross-Site Request Forgery (CSRF) vulnerability in Glen Don L. Mongaya Drag and Drop Multiple File Upload – Contact Form 7 plugin <= 1.3.6.5 versions.	5.4	More Detail
CVE-2023-33943	Cross-site scripting (XSS) vulnerability in the Account module in Liferay Portal 7.4.3.21 through 7.4.3.62, and Liferay DXP 7.4 update 21 through 62 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user's (1) First Name, (2) Middle Name, (3) Last Name, or (4) Job Title text field.	5.4	More Detail
CVE-2022-24631	An issue was discovered in AudioCodes Device Manager Express through 7.8.20002.47752. It is stored XSS via the ajaxTenants.php desc parameter.	5.4	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-33942	Cross-site scripting (XSS) vulnerability in the Web Content Display widget's article selector in Liferay Liferay Portal 7.4.3.50, and Liferay DXP 7.4 update 50 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a web content article's `Title` field.	5.4	More Detail
CVE-2023-25467	Cross-Site Request Forgery (CSRF) vulnerability in Daniel Mores, A. Huizinga Resize at Upload Plus plugin <= 1.3 versions.	5.4	More Detail
CVE-2023-33394	skycaiji v2.5.4 is vulnerable to Cross Site Scripting (XSS). Attackers can achieve backend XSS by deploying malicious JSON data.	5.4	More Detail
CVE-2023-33939	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4 before update 9 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label.	5.4	More Detail
CVE-2023-33937	Stored cross-site scripting (XSS) vulnerability in Form widget configuration in Liferay Portal 7.1.0 through 7.3.0, and Liferay DXP 7.1 before fix pack 18, and 7.2 before fix pack 5 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a form's `name` field.	5.4	More Detail
CVE-2023-2954	Cross-site Scripting (XSS) - Stored in GitHub repository liangliangyy/djangoblog prior to master.	5.4	More Detail
CVE-2022-47446	Cross-Site Request Forgery (CSRF) vulnerability in Viadat Creations Store Locator for WordPress with Google Maps – LotsOfLocales plugin <= 3.98.7 versions.	5.4	More Detail
CVE-2023-33315	Cross-Site Request Forgery (CSRF) vulnerability in Stephen Darlington, Wandle Software Limited Smart App Banner plugin <= 1.1.2 versions.	5.4	More Detail
CVE-2023-33791	A stored cross-site scripting (XSS) vulnerability in the Create Provider Accounts (/circuits/provider-accounts/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33829	A stored cross-site scripting (XSS) vulnerability in Cloudogu GmbH SCM Manager v1.2 to v1.60 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description text field.	5.4	More Detail
CVE-2023-23956	A user can supply malicious HTML and JavaScript code that will be executed in the client browser	5.4	More Detail
CVE-2023-32325	PostHog-js is a library to interface with the PostHog analytics tool. Versions prior to 1.57.2 have the potential for cross-site scripting. Problem has been patched in 1.57.2. Users are advised to upgrade. Users unable to upgrade should ensure that their Content Security Policy is in place.	5.4	More Detail
CVE-2022-45371	Cross-Site Request Forgery (CSRF) vulnerability in Wpmet ShopEngine plugin <= 4.1.1 versions.	5.4	More Detail
CVE-2022-43490	Cross-Site Request Forgery (CSRF) vulnerability in XWP Stream plugin <= 3.9.2 versions.	5.4	More Detail
CVE-2022-38716	Cross-Site Request Forgery (CSRF) vulnerability in StylemixThemes Motors – Car Dealer, Classifieds & Listing plugin <= 1.4.4 versions.	5.4	More Detail
CVE-2022-36249	Shop Beat Solutions (Pty) LTD Shop Beat Media Player 2.5.95 up to 3.2.57 is vulnerable to Bypass 2FA via APIs. For Controlpanel Lite. "After login we are directly able to use the bearer token or jsession ID to access the apis instead of entering the 2FA code. Thus, leading to bypass of 2FA on API level.	5.4	More Detail
CVE-2022-38356	Cross-Site Request Forgery (CSRF) vulnerability in StylemixThemes WordPress Header Builder Plugin – Pearl plugin <= 1.3.4 versions.	5.4	More Detail
CVE-2022-36244	Shop Beat Solutions (Pty) LTD Shop Beat Media Player 2.5.95 up to 3.2.57 suffers from Multiple Stored Cross-Site Scripting (XSS) vulnerabilities via Shop Beat Control Panel found at www.shopbeat.co.za controlpanel.shopbeat.co.za.	5.4	More Detail
CVE-2023-33356	IceCMS v1.0.0 is vulnerable to Cross Site Scripting (XSS).	5.4	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-4676	The OSM WordPress plugin through 6.01 does not validate and escape some of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Detail
CVE-2023-2926	A vulnerability was found in SeaCMS 11.6 and classified as problematic. This issue affects some unknown processing of the file member.php of the component Picture Upload Handler. The manipulation of the argument oldpic leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-230081 was assigned to this vulnerability.	5.4	More Detail
CVE-2022-47139	Cross-Site Request Forgery (CSRF) vulnerability in Damir Calusic WP Basic Elements plugin <= 5.2.15 versions.	5.4	More Detail
CVE-2022-46820	Cross-Site Request Forgery (CSRF) vulnerability in WPJoli Joli Table Of Contents plugin <= 1.3.9 versions.	5.4	More Detail
CVE-2023-33780	A stored cross-site scripting (XSS) vulnerability in TFDi Design smartCARS 3 v0.7.0 and below allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the body of news article.	5.4	More Detail
CVE-2022-46800	Cross-Site Request Forgery (CSRF) vulnerability in LiteSpeed Technologies LiteSpeed Cache plugin <= 5.3 versions.	5.4	More Detail
CVE-2023-33800	A stored cross-site scripting (XSS) vulnerability in the Create Regions (/dcim/regions/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33751	A stored cross-site scripting (XSS) vulnerability in mipjz v5.0.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter at /app/tag/controller/ApiAdminTagCategory.php.	5.4	More Detail
CVE-2023-33314	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 BEAR plugin <= 1.1.3.1 versions.	5.4	More Detail
CVE-2023-33792	A stored cross-site scripting (XSS) vulnerability in the Create Site Groups (/dcim/site-groups/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33187	Highlight is an open source, full-stack monitoring platform. Highlight may record passwords on customer deployments when a password html input is switched to `type="text"` via a javascript "Show Password" button. This differs from the expected behavior which always obfuscates `type="password"` inputs. A customer may assume that switching to `type="text"` would also not record this input; hence, they would not add additional `highlight-mask` css-class obfuscation to this part of the DOM, resulting in unintentional recording of a password value when a `Show Password` button is used. This issue was patched in version 6.0.0. This patch tracks changes to the `type` attribute of an input to ensure an input that used to be a `type="password"` continues to be obfuscated.	5.4	More Detail
CVE-2023-33793	A stored cross-site scripting (XSS) vulnerability in the Create Power Panels (/dcim/power-panels/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33794	A stored cross-site scripting (XSS) vulnerability in the Create Tenants (/tenancy/tenants/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33795	A stored cross-site scripting (XSS) vulnerability in the Create Contact Roles (/tenancy/contact-roles/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-33797	A stored cross-site scripting (XSS) vulnerability in the Create Sites (/dcim/sites/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-2817	A post-authentication stored cross-site scripting vulnerability exists in Craft CMS versions <= 4.4.11. HTML, including script tags can be injected into field names which, when the field is added to a category or section, will trigger when users visit the Categories or Entries pages respectively.	5.4	More Detail
CVE-2023-2944	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.1.	5.4	More Detail
CVE-2023-33750	A stored cross-site scripting (XSS) vulnerability in mipjz v5.0.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description parameter at /index.php?s=/article/ApiAdminArticle/itemAdd.	5.4	More Detail
CVE-2023-33798	A stored cross-site scripting (XSS) vulnerability in the Create Rack (/dcim/rack/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-33799	A stored cross-site scripting (XSS) vulnerability in the Create Contacts (/tenancy/contacts/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Detail
CVE-2023-2945	Missing Authorization in GitHub repository openemr/openemr prior to 7.0.1.	5.4	More Detail
CVE-2022-24632	An issue was discovered in AudioCodes Device Manager Express through 7.8.20002.47752. It is directory traversal during file download via the BrowseFiles.php view parameter.	5.3	More Detail
CVE-2023-31186	Avaya IX Workforce Engagement v15.2.7.1195 - User Enumeration - Observable Response Discrepancy	5.3	More Detail
CVE-2022-36243	Shop Beat Solutions (pty) LTD Shop Beat Media Player 2.5.95 up to 3.2.57 is vulnerable to Directory Traversal via server.shopbeat.co.za. Information Exposure Through Directory Listing vulnerability in "studio" software of Shop Beat. This issue affects: Shop Beat studio studio versions prior to 3.2.57 on arm.	5.3	More Detail
CVE-2023-0443	The AnyWhere Elementor WordPress plugin before 1.2.8 discloses a Freemius Secret Key which could be used by an attacker to purchase the pro subscription using test credit card numbers without actually paying the amount. Such key has been revoked.	5.3	More Detail
CVE-2023-2952	XRA dissector infinite loop in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via packet injection or crafted capture file	5.3	More Detail
CVE-2023-2854	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file	5.3	More Detail
CVE-2023-0117	The online authentication provided by the hwKitAssistant lacks strict identity verification of applications. Successful exploitation of this vulnerability may affect availability of features,such as MeeTime.	5.3	More Detail
CVE-2023-32762	An issue was discovered in Qt before 5.15.14, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. Qt Network incorrectly parses the strict-transport-security (HSTS) header, allowing unencrypted connections to be established, even when explicitly prohibited by the server. This happens if the case used for this header does not exactly match.	5.3	More Detail
CVE-2023-33199	Rekor's goals are to provide an immutable tamper resistant ledger of metadata generated within a software projects supply chain. A malformed proposed entry of the `intoto/v0.0.2` type can cause a panic on a thread within the Rekor process. The thread is recovered so the client receives a 500 error message and service still continues, so the availability impact of this is minimal. This has been fixed in v1.2.0 of Rekor. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Detail
CVE-2023-27311	NetApp Blue XP Connector versions prior to 3.9.25 expose information via a directory listing. A new Connector architecture resolves this issue - obtaining the fix requires redeploying a fresh Connector.	5.3	More Detail
CVE-2023-33948	The Dynamic Data Mapping module in Liferay Portal 7.4.3.67, and Liferay DXP 7.4 update 67 does not limit Document and Media files which can be downloaded from a Form, which allows remote attackers to download any file from Document and Media via a crafted URL.	5.3	More Detail
CVE-2023-33949	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.2 and earlier the default configuration does not require users to verify their email address, which allows remote attackers to create accounts using fake email addresses or email addresses which they don't control. The portal property `company.security.strangers.verify` should be set to true.	5.3	More Detail
CVE-2023-2873	A vulnerability classified as critical was found in Twister Antivirus 8. This vulnerability affects the function 0x804f2143/0x804f217f/0x804f214b/0x80800043 in the library filppd.sys of the component IoControlCode Handler. The manipulation leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Detail
CVE-2023-2858	NetScaler file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file	5.3	More Detail
CVE-2023-2857	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file	5.3	More Detail
CVE-2023-2856	VMS TCPIPtrace file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file	5.3	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-2255	Improper access control in editor components of The Document Foundation LibreOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. In the affected versions of LibreOffice documents that used "floating frames" linked to external files, would load the contents of those frames without prompting the user for permission to do so. This was inconsistent with the treatment of other linked content in LibreOffice. This issue affects: The Document Foundation LibreOffice 7.4 versions prior to 7.4.7; 7.5 versions prior to 7.5.3.	5.3	More Detail
CVE-2023-2855	Candump log parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file	5.3	More Detail
CVE-2023-24597	OX App Suite before frontend 7.10.6-rev24 allows the loading (without user consent) of an e-mail message's remote resources during printing.	5.3	More Detail
CVE-2023-33195	Craft is a CMS for creating custom digital experiences on the web. A malformed RSS feed can deliver an XSS payload. This issue was patched in version 4.4.6.	5.0	More Detail
CVE-2023-24568	Dell NetWorker, contains an Improper Validation of Certificate with Host Mismatch vulnerability in Rabbitmq port which could disallow replacing CA signed certificates.	5.0	More Detail
CVE-2023-32323	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. A malicious user on a Synapse homeserver X with permission to create certain state events can disable outbound federation from X to an arbitrary homeserver Y. Synapse instances with federation disabled are not affected. In versions of Synapse up to and including 1.73, Synapse did not limit the size of `invite_room_state`, meaning that it was possible to create an arbitrarily large invite event. Synapse 1.74 refuses to create oversized `invite_room_state` fields. Server operators should upgrade to Synapse 1.74 or newer urgently.	5.0	More Detail
CVE-2022-39335	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. The Matrix Federation API allows remote homeservers to request the authorization events in a room. This is necessary so that a homeserver receiving some events can validate that those events are legitimate and permitted in their room. However, in versions of Synapse up to and including 1.68.0, a Synapse homeserver answering a query for authorization events does not sufficiently check that the requesting server should be able to access them. The issue was patched in Synapse 1.69.0. Homeserver administrators are advised to upgrade.	5.0	More Detail
CVE-2023-2111	The Fast & Effective Popups & Lead-Generation for WordPress plugin before 2.1.4 concatenates user input into an SQL query without escaping it first in the plugin's report API endpoint, which could allow administrators in multi-site configuration to leak sensitive information from the site's database.	4.9	More Detail
CVE-2023-32688	parse-server-push-adapter is the official Push Notification adapter for Parse Server. The Parse Server Push Adapter can crash Parse Server due to an invalid push notification payload. This issue has been patched in version 4.1.3.	4.9	More Detail
CVE-2023-2881	Storing Passwords in a Recoverable Format in GitHub repository pimcore/customer-data-framework prior to 3.3.10.	4.9	More Detail
CVE-2023-33938	Cross-site scripting (XSS) vulnerability in the App Builder module's custom object details page in Liferay Portal 7.3.0 through 7.4.0, and Liferay DXP 7.3 before update 14 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an App Builder custom object's `Name` field.	4.8	More Detail
CVE-2023-2947	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.1.	4.8	More Detail
CVE-2023-33940	Cross-site scripting (XSS) vulnerability in IFrame type Remote Apps in Liferay Portal 7.4.0 through 7.4.3.30, and Liferay DXP 7.4 before update 31 allows remote attackers to inject arbitrary web script or HTML via the Remote App's IFrame URL.	4.8	More Detail
CVE-2023-33944	Cross-site scripting (XSS) vulnerability in Layout module in Liferay Portal 7.3.4 through 7.4.3.68, and Liferay DXP 7.3 before update 24, and 7.4 before update 69 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a container type layout fragment's `URL` text field.	4.8	More Detail
CVE-2023-2113	The Autoptimize WordPress plugin before 3.1.7 does not sanitise and escape the settings imported from a previous export, allowing high privileged users (such as an administrator) to inject arbitrary javascript into the admin panel, even when the unfiltered_html capability is disabled, such as in a multisite setup.	4.8	More Detail
CVE-2023-2223	The Login rebuilder WordPress plugin before 2.8.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Detail
CVE-2023-2470	The Add to Feedly WordPress plugin through 1.2.11 does not sanitize and escape its settings, allowing high-privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Detail
CVE-2023-32694	Saleor Core is a composable, headless commerce API. Saleor's `validate_hmac_signature` function is vulnerable to timing attacks. Malicious users could abuse this vulnerability on Saleor deployments having the Adyen plugin enabled in order to determine the secret key and forge fake events, this could affect the database integrity such as marking an order as paid when it is not. This issue has been patched in versions 3.7.68, 3.8.40, 3.9.49, 3.10.36, 3.11.35, 3.12.25, and 3.13.16.	4.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-32072	Tuleap is an open source tool for end to end traceability of application and system developments. Tuleap Community Edition prior to version 14.8.99.60 and Tuleap Enterprise edition prior to 14.8-3 and 14.7-7, the logs of the triggered Jenkins job URLs are not properly escaped. A malicious Git administrator can setup a malicious Jenkins hook to make a victim, also a Git administrator, execute uncontrolled code. Tuleap Community Edition 14.8.99.60, Tuleap Enterprise Edition 14.8-3, and Tuleap Enterprise Edition 14.7-7 contain a patch for this issue.	4.8	More Detail
CVE-2023-2979	A vulnerability classified as critical has been found in Abstrium Pydio Cells 4.2.0. This affects an unknown part of the component User Creation Handler. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.2.1 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-230211.	4.7	More Detail
CVE-2023-2898	There is a null-pointer-dereference flaw found in f2fs_write_end_io in fs/f2fs/data.c in the Linux kernel. This flaw allows a local privileged user to cause a denial of service problem.	4.7	More Detail
CVE-2023-2924	A vulnerability, which was classified as critical, has been found in Supcon SimField up to 1.80.00.00. Affected by this issue is some unknown functionality of the file /admin/reportupload.aspx. The manipulation of the argument files[] leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-230078 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Detail
CVE-2023-2888	A vulnerability, which was classified as problematic, was found in PHPOK 6.4.100. This affects an unknown part of the file /admin.php?c=upload&f=zip&_noCache=0.1683794968. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The identifier VDB-229953 was assigned to this vulnerability.	4.7	More Detail
CVE-2023-2962	A vulnerability, which was classified as critical, has been found in SourceCodester Faculty Evaluation System 1.0. Affected by this issue is some unknown functionality of the file index.php?page=edit_user. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-230150 is the identifier assigned to this vulnerability.	4.7	More Detail
CVE-2023-2494	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'process_postdata' function in versions up to, and including, 3.3.19. This makes it possible for authenticated attackers with a role that the administrator previously granted access to the plugin to modify access to the plugin when it should only be the administrator's privilege.	4.6	More Detail
CVE-2023-33185	Django-SES is a drop-in mail backend for Django. The django_ses library implements a mail backend for Django using AWS Simple Email Service. The library exports the `SESEventWebhookView class` intended to receive signed requests from AWS to handle email bounces, subscriptions, etc. These requests are signed by AWS and are verified by django_ses, however the verification of this signature was found to be flawed as it allowed users to specify arbitrary public certificates. This issue was patched in version 3.5.0.	4.6	More Detail
CVE-2023-33191	Kyverno is a policy engine designed for Kubernetes. Kyverno seccomp control can be circumvented. Users of the podSecurity `validate.podSecurity` subrule in Kyverno 1.9.2 and 1.9.3 are vulnerable. This issue was patched in version 1.9.4.	4.6	More Detail
CVE-2023-2978	A vulnerability was found in Abstrium Pydio Cells 4.2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Change Subscription Handler. The manipulation leads to authorization bypass. The exploit has been disclosed to the public and may be used. Upgrading to version 4.2.1 is able to address this issue. It is recommended to upgrade the affected component. VDB-230210 is the identifier assigned to this vulnerability.	4.6	More Detail
CVE-2023-32685	Kanboard is project management software that focuses on the Kanban methodology. Due to improper handling of elements under the `contentEditable` element, maliciously crafted clipboard content can inject arbitrary HTML tags into the DOM. A low-privileged attacker with permission to attach a document on a vulnerable Kanboard instance can trick the victim into pasting malicious screenshot data and achieve cross-site scripting if CSP is improperly configured. This issue has been patched in version 1.2.29.	4.4	More Detail
CVE-2023-24604	OX App Suite before backend 7.10.6-rev37 does not check HTTP header lengths when downloading, e.g., potentially allowing a crafted iCal feed to provide an unlimited amount of header data.	4.3	More Detail
CVE-2022-47174	Cross-Site Request Forgery (CSRF) vulnerability in WordPress Performance Team Performance Lab plugin <= 2.2.0 versions.	4.3	More Detail
CVE-2023-24600	OX App Suite before backend 7.10.6-rev37 allows authenticated users to bypass access controls (for reading contacts) via a move to their own address book.	4.3	More Detail
CVE-2023-24598	OX App Suite before backend 7.10.6-rev37 has an information leak in the handling of distribution lists, e.g., partial disclosure of the private contacts of another user.	4.3	More Detail
CVE-2022-41766	An issue was discovered in MediaWiki before 1.35.8, 1.36.x and 1.37.x before 1.37.5, and 1.38.x before 1.38.3. Upon an action=rollback operation, the alreadyrolled message can leak a user name (when the user has been revision deleted/suppressed).	4.3	More Detail
CVE-2023-33955	Minio Console is the UI for MinIO Object Storage. Unicode RIGHT-TO-LEFT OVERRIDE characters can be used to mask the original filename. This issue has been patched in version 0.28.0.	4.3	More Detail

CVE Number	Description	Base Score	Refer
CVE-2014-125102	A vulnerability classified as problematic was found in Bestwebsoft Relevant Plugin up to 1.0.7 on WordPress. Affected by this vulnerability is an unknown functionality of the component Thumbnail Handler. The manipulation leads to information disclosure. The attack can be launched remotely. Upgrading to version 1.0.8 is able to address this issue. The identifier of the patch is 860d1891025548cf0f5f97364c1f51a888f523c3. It is recommended to upgrade the affected component. The identifier VDB-230113 was assigned to this vulnerability.	4.3	More Detail
CVE-2022-45372	Cross-Site Request Forgery (CSRF) vulnerability in Codeixer Product Gallery Slider for WooCommerce plugin <= 2.2.8 versions.	4.3	More Detail
CVE-2022-36345	Cross-Site Request Forgery (CSRF) vulnerability in Metagauss Download Plugin <= 2.0.4 versions.	4.3	More Detail
CVE-2023-33313	Cross-Site Request Forgery (CSRF) vulnerability in ThemeinProgress WIP Custom Login plugin <= 1.2.9 versions.	4.3	More Detail
CVE-2023-33931	Cross-Site Request Forgery (CSRF) vulnerability in Ciprian Popescu YouTube Playlist Player plugin <= 4.6.4 versions.	4.3	More Detail
CVE-2023-2902	A vulnerability was found in NFine Rapid Development Platform 20230511. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /SystemManage/Organize/GetTreeGridJson?_search=false&nd=1681813520783&rows=10000&page=1&sidx=&sord=asc. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229976. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Detail
CVE-2023-33212	Cross-Site Request Forgery (CSRF) vulnerability in Crocoblock JetFormBuilder — Dynamic Blocks Form Builder plugin <= 3.0.6 versions.	4.3	More Detail
CVE-2023-2901	A vulnerability was found in NFine Rapid Development Platform 20230511. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /SystemManage/User/GetGridJson?_search=false&nd=1680855479750&rows=50&page=1&sidx=F_CreatorTime+desc&sord=asc. The manipulation leads to improper access controls. 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-229975. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Detail
CVE-2023-2903	A vulnerability classified as problematic has been found in NFine Rapid Development Platform 20230511. This affects an unknown part of the file /SystemManage/Role/GetGridJson?keyword=&page=1&rows=20. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229977 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Detail
CVE-2022-47144	Cross-Site Request Forgery (CSRF) vulnerability in Plugincraft Mediamatic – Media Library Folders plugin <= 2.8.1 versions.	4.3	More Detail
CVE-2023-2808	Mattermost fails to normalize UTF confusable characters when determining if a preview should be generated for a hyperlink, allowing an attacker to trigger link preview on a disallowed domain using a specially crafted link.	4.3	More Detail
CVE-2023-23714	Cross-Site Request Forgery (CSRF) vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash plugin <= 3.6.4.1 versions.	4.3	More Detail
CVE-2023-24007	Cross-Site Request Forgery (CSRF) vulnerability in TheOnlineHero - Tom Skroza Admin Block Country plugin <= 7.1.4 versions.	4.3	More Detail
CVE-2023-25971	Cross-Site Request Forgery (CSRF) vulnerability in FixBD Educare plugin <= 1.4.1 versions.	4.3	More Detail
CVE-2023-25976	Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks Integration for Contact Form 7 and Zoho CRM, Bigin plugin <= 1.2.2 versions.	4.3	More Detail
CVE-2023-22693	Cross-Site Request Forgery (CSRF) vulnerability in conlabzgmbh WP Google Tag Manager plugin <= 1.1 versions.	4.3	More Detail
CVE-2023-24008	Cross-Site Request Forgery (CSRF) vulnerability in yonifre Maspik – Spam Blacklist plugin <= 0.7.8 versions.	4.3	More Detail
CVE-2023-25038	Cross-Site Request Forgery (CSRF) vulnerability in 984.Ru For the visually impaired plugin <= 0.58 versions.	4.3	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-2287	The Orbit Fox by ThemeIsle WordPress plugin before 2.10.24 does not limit URLs which may be used for the stock photo import feature, allowing the user to specify arbitrary URLs. This leads to a server-side request forgery as the user may force the server to access any URL of their choosing.	4.3	More Detail
CVE-2023-25029	Cross-Site Request Forgery (CSRF) vulnerability in utahta WP Social Bookmarking Light plugin <= 2.0.7 versions.	4.3	More Detail
CVE-2023-25470	Cross-Site Request Forgery (CSRF) vulnerability in Anton Skorobogatov Rus-To-Lat plugin <= 0.3 versions.	4.3	More Detail
CVE-2023-25034	Cross-Site Request Forgery (CSRF) vulnerability in BoLiQuan WP Clean Up plugin <= 1.2.3 versions.	4.3	More Detail
CVE-2023-25058	Cross-Site Request Forgery (CSRF) vulnerability in Brainstorm Force Schema – All In One Schema Rich Snippets plugin <= 1.6.5 versions.	4.3	More Detail
CVE-2023-32964	Cross-Site Request Forgery (CSRF) vulnerability in Made with Fuel Better Notifications for WP plugin <= 1.9.2 versions.	4.3	More Detail
CVE-2022-47178	Cross-Site Request Forgery (CSRF) vulnerability in Simple Share Buttons Simple Share Buttons Adder plugin <= 8.4.7 versions.	4.3	More Detail
CVE-2023-24599	OX App Suite before backend 7.10.6-rev37 allows authenticated users to change the appointments of arbitrary users via conflicting ID numbers, aka "ID confusion."	4.3	More Detail
CVE-2022-47136	Cross-Site Request Forgery (CSRF) vulnerability in WPManageNinja LLC Ninja Tables – Best Data Table Plugin for WordPress plugin <= 4.3.4 versions.	4.3	More Detail
CVE-2022-41635	Cross-Site Request Forgery (CSRF) vulnerability in Zorem Advanced Shipment Tracking for WooCommerce plugin <= 3.5.2 versions.	4.3	More Detail
CVE-2023-2937	Inappropriate implementation in Picture In Picture in Google Chrome prior to 114.0.5735.90 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Detail
CVE-2022-46812	Cross-Site Request Forgery (CSRF) vulnerability in VillaTheme Thank You Page Customizer for WooCommerce – Increase Your Sales plugin <= 1.0.13 versions.	4.3	More Detail
CVE-2022-46865	Cross-Site Request Forgery (CSRF) vulnerability in Marty Thornley Bulk Resize Media plugin <= 1.1 versions.	4.3	More Detail
CVE-2022-46866	Cross-Site Request Forgery (CSRF) vulnerability in Marty Thornley Import External Images plugin <= 1.4 versions.	4.3	More Detail
CVE-2022-46814	Cross-Site Request Forgery (CSRF) vulnerability in Pierre Lebedel Kodex Posts likes plugin <= 2.4.3 versions.	4.3	More Detail
CVE-2023-2938	Inappropriate implementation in Picture In Picture in Google Chrome prior to 114.0.5735.90 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Detail
CVE-2023-2941	Inappropriate implementation in Extensions API in Google Chrome prior to 114.0.5735.90 allowed an attacker who convinced a user to install a malicious extension to spoof the contents of the UI via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Detail
CVE-2023-33181	Xibo is a content management system (CMS). Starting in version 3.0.0 and prior to version 3.3.5, some API routes will print a stack trace when called with missing or invalid parameters revealing sensitive information about the locations of paths that the server is using. Users should upgrade to version 3.3.5, which fixes this issue. There are no known workarounds aside from upgrading.	4.3	More Detail
CVE-2022-47135	Cross-Site Request Forgery (CSRF) vulnerability in chronoengine.Com Chronoforms plugin <= 7.0.9 versions.	4.3	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-47138	Cross-Site Request Forgery (CSRF) vulnerability in German Krutov LOGIN AND REGISTRATION ATTEMPTS LIMIT plugin <= 2.1 versions.	4.3	More Detail
CVE-2022-47159	Cross-Site Request Forgery (CSRF) vulnerability in Logaster Logaster Logo Generator plugin <= 1.3 versions.	4.3	More Detail
CVE-2022-47164	Cross-Site Request Forgery (CSRF) vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin for WooCommerce plugin <= 3.7.7 versions.	4.3	More Detail
CVE-2023-2886	Missing Origin Validation in WebSockets vulnerability in CBOT Chatbot allows Content Spoofing Via Application API Manipulation.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.	4.3	More Detail
CVE-2022-47447	Cross-Site Request Forgery (CSRF) vulnerability in Mathieu Chartier WordPress WP-Advanced-Search plugin <= 3.3.8 versions.	4.3	More Detail
CVE-2022-45367	Cross-Site Request Forgery (CSRF) vulnerability in Tyche Softwares Custom Order Numbers for WooCommerce plugin <= 1.4.0 versions.	4.3	More Detail
CVE-2022-47149	Cross-Site Request Forgery (CSRF) vulnerability in Pretty Links plugin <= 3.4.0 versions.	4.3	More Detail
CVE-2022-47161	Cross-Site Request Forgery (CSRF) vulnerability in The WordPress.Org community Health Check & Troubleshooting plugin <= 1.5.1 versions.	4.3	More Detail
CVE-2022-47165	Cross-Site Request Forgery (CSRF) vulnerability in CoSchedule plugin <= 3.3.8 versions.	4.3	More Detail
CVE-2022-47180	Cross-Site Request Forgery (CSRF) vulnerability in Kopa Theme Kopa Framework plugin <= 1.3.5 versions.	4.3	More Detail
CVE-2022-47177	Cross-Site Request Forgery (CSRF) vulnerability in WP Easy Pay WP EasyPay – Square for WordPress plugin <= 4.1 versions.	4.3	More Detail
CVE-2022-46816	Cross-Site Request Forgery (CSRF) vulnerability in Booking Ultra Pro Appointments Booking Calendar Plugin plugin <= 1.1.4 versions.	4.3	More Detail
CVE-2023-30484	Cross-Site Request Forgery (CSRF) vulnerability in uPress Enable Accessibility plugin <= 1.4 versions.	4.3	More Detail
CVE-2022-45815	Cross-Site Request Forgery (CSRF) vulnerability in StylemixThemes GDPR Compliance & Cookie Consent plugin <= 1.2 versions.	4.3	More Detail
CVE-2022-46794	Cross-Site Request Forgery (CSRF) vulnerability in weightbasedshipping.Com WooCommerce Weight Based Shipping plugin <= 5.4.1 versions.	4.3	More Detail
CVE-2022-46810	Cross-Site Request Forgery (CSRF) vulnerability in VillaTheme Thank You Page Customizer for WooCommerce – Increase Your Sales plugin <= 1.0.13 versions.	4.3	More Detail
CVE-2023-1158	Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.1 and 9.3.0.3, including 8.3.x expose dashboard prompts to users who are not part of the authorization list.	4.3	More Detail
CVE-2023-24605	OX App Suite before backend 7.10.6-rev37 does not enforce 2FA for all endpoints, e.g., reading from a drive, reading contact data, and renaming tokens.	4.2	More Detail
CVE-2023-31130	c-ares is an asynchronous resolver library. ares_inet_net_pton() is vulnerable to a buffer underflow for certain ipv6 addresses, in particular "0::00:00:00/2" was found to cause an issue. C-ares only uses this function internally for configuration purposes which would require an administrator to configure such an address via ares_set_sortlist(). However, users may externally use ares_inet_net_pton() for other purposes and thus be vulnerable to more severe issues. This issue has been fixed in 1.19.1.	4.1	More Detail

CVE Number	Description	Base Score	Refer
CVE-2023-1711	A vulnerability exists in a FOXMAN-UN and UNEM logging component, it only affects systems that use remote authentication to the network elements. If exploited an attacker could obtain confidential information. List of CPEs: * cpe:2.3:a:hitachienergy:foxman_un:R9C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R10C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R11A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R11B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R14A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R14B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R15A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R15B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman_un:R16A:*:*:*:*:*:*:* * * cpe:2.3:a:hitachienergy:unem:R9C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R10C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R11A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R11B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R14A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R14B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R15A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R15B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy: unem :R16A:*:*:*:*:*:*:*	4.0	More Detail
CVE-2023-30571	Libarchive through 3.6.2 can cause directories to have world-writable permissions. The umask() call inside archive_write_disk_posix.c changes the umask of the whole process for a very short period of time; a race condition with another thread can lead to a permanent umask 0 setting. Such a race condition could lead to implicit directory creation with permissions 0777 (without the sticky bit), which means that any low-privileged local user can delete and rename files inside those directories.	3.9	More Detail
CVE-2023-33194	Craft is a CMS for creating custom digital experiences on the web.The platform does not filter input and encode output in Quick Post validation error message, which can deliver an XSS payload. Old CVE fixed the XSS in label HTML but didn't fix it when clicking save. This issue was patched in version 4.4.6.	3.7	More Detail
CVE-2023-28322	An information disclosure vulnerability exists in curl <v8.1.0 when doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set, if the same handle previously wasused to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST.	3.7	More Detail
CVE-2021-37845	An issue was discovered in Citadel through webcit-932. A meddler-in-the-middle attacker can fixate their own session during the cleartext phase before a STARTTLS command (a violation of "The STARTTLS command is only valid in non-authenticated state." in RFC2595). This potentially allows an attacker to cause a victim's e-mail messages to be stored into an attacker's IMAP mailbox, but depends on details of the victim's client behavior.	3.7	More Detail
CVE-2023-31124	c-ares is an asynchronous resolver library. When cross-compiling c-ares and using the autotools build system, CARES_RANDOM_FILE will not be set, as seen when cross compiling aarch64 android. This will downgrade to using rand() as a fallback which could allow an attacker to take advantage of the lack of entropy by not using a CSPRNG. This issue was patched in version 1.19.1.	3.7	More Detail
CVE-2023-2900	A vulnerability was found in NFine Rapid Development Platform 20230511. It has been classified as problematic. Affected is an unknown function of the file /Login/CheckLogin. The manipulation leads to use of weak hash. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. VDB-229974 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Detail
CVE-2023-33184	Nextcloud Mail is a mail app in Nextcloud. A blind SSRF attack allowed to send GET requests to services running in the same web server. It is recommended that the Mail app is update to version 3.02, 2.2.5 or 1.15.3.	3.5	More Detail
CVE-2023-2970	A vulnerability classified as problematic was found in MindSpore 2.0.0-alpha/2.0.0-rc1. This vulnerability affects the function JsonHelper::UpdateArray of the file mindspore/ccsrc/minddata/dataset/util/json_helper.cc. The manipulation leads to memory corruption. The name of the patch is 30f4729ea2c01e1ed437ba92a81e2fc098d608a9. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-230176.	3.5	More Detail
CVE-2023-2862	A vulnerability, which was classified as problematic, was found in SiteServer CMS up to 7.2.1. Affected is an unknown function of the file /api/stl/actions/search. The manipulation of the argument ajaxDivId 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. It is recommended to apply a patch to fix this issue. VDB-229818 is the identifier assigned to this vulnerability.	3.5	More Detail
CVE-2023-2981	A vulnerability, which was classified as problematic, has been found in Abstrium Pydio Cells 4.2.0. This issue affects some unknown processing of the component Chat. The manipulation leads to basic cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.2.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-230213 was assigned to this vulnerability.	3.5	More Detail
CVE-2023-2922	A vulnerability classified as problematic has been found in SourceCodester Comment System 1.0. Affected is an unknown function of the file index.php of the component GET Parameter Handler. The manipulation of the argument msg 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-230076.	3.5	More Detail
CVE-2023-2864	A vulnerability was found in SourceCodester Online Jewelry Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file customer.php of the component POST Parameter Handler. The manipulation of the argument Custid leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229820.	3.5	More Detail
CVE-2023-2871	A vulnerability was found in FabulaTech USB for Remote Desktop 6.1.0.0. It has been rated as problematic. Affected by this issue is the function 0x220448/0x220420/0x22040c/0x220408 of the component IoControlCode Handler. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-229850 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Detail
CVE-2023-2870	A vulnerability was found in EnTech Monitor Asset Manager 2.9. It has been declared as problematic. Affected by this vulnerability is the function 0x80002014 of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier VDB-229849 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-39074	There is an unauthorized access vulnerability in some ZTE mobile phones. If a malicious application is installed on the phone, it could start a non-public interface of an application without user permission.	3.3	More Detail
CVE-2023-31225	The Gallery app has the risk of hijacking attacks. Successful exploitation of this vulnerability may cause download failures and affect product availability.	3.3	More Detail
CVE-2023-33947	The Object module in Liferay Portal 7.4.3.4 through 7.4.3.60, and Liferay DXP 7.4 before update 61 does not segment object definition by virtual instance in search which allows remote authenticated users in one virtual instance to view object definition from a second virtual instance by searching for the object definition.	2.7	More Detail
CVE-2023-33946	The Object module in Liferay Portal 7.4.3.4 through 7.4.3.48, and Liferay DXP 7.4 before update 49 does properly isolate objects in difference virtual instances, which allows remote authenticated users in one virtual instance to view objects in a different virtual instance via OAuth 2 scope administration page.	2.7	More Detail
CVE-2023-32684	Lima launches Linux virtual machines, typically on macOS, for running containerd. Prior to version 0.16.0, a virtual machine instance with a malicious disk image could read a single file on the host filesystem, even when no filesystem is mounted from the host. The official templates of Lima and the well-known third party products (Colima, Rancher Desktop, and Finch) are unlikely to be affected by this issue. To exploit this issue, the attacker has to embed the target file path (an absolute or a relative path from the instance directory) in a malicious disk image, as the qcow2 (or vmdk) backing file path string. As Lima refuses to run as the root, it is practically impossible for the attacker to read the entire host disk via `/dev/rdiskN`. Also, practically, the attacker cannot read at least the first 512 bytes (MBR) of the target file. The issue has been patched in Lima in version 0.16.0 by prohibiting using a backing file path in the VM base image.	2.7	More Detail
CVE-2023-2117	The Image Optimizer by 10web WordPress plugin before 1.0.27 does not sanitize the dir parameter when handling the get_subdirs ajax action, allowing a high privileged users such as admins to inspect names of files and directories outside of the sites root.	2.7	More Detail
CVE-2023-30851	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. This issue only impacts users who have a HTTP policy that applies to multiple `toEndpoints` AND have an allow-all rule in place that affects only one of those endpoints. In such cases, a wildcard rule will be appended to the set of HTTP rules, which could cause bypass of HTTP policies. This issue has been patched in Cilium 1.11.16, 1.12.9, and 1.13.2.	2.6	More Detail
CVE-2023-33183	Calendar app for Nextcloud easily sync events from various devices with your Nextcloud. Some internal paths of the website are disclosed when the SMTP server is unavailable. It is recommended that the Calendar app is updated to 3.5.5 or 4.2.3	2.6	More Detail
CVE-2023-2973	A vulnerability, which was classified as problematic, has been found in SourceCodester Students Online Internship Timesheet Syste 1.0. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_company. The manipulation of the argument name with the input <script>alert(document.cookie)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230204.	2.4	More Detail
CVE-2023-2925	A vulnerability, which was classified as problematic, was found in Webkul krayin crm 1.2.4. This affects an unknown part of the file /admin/contacts/organizations/edit/2 of the component Edit Person Page. The manipulation of the argument Organization 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-230079. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Detail
CVE-2023-2863	A vulnerability has been found in Simple Design Daily Journal 1.012.GP.B on Android and classified as problematic. Affected by this vulnerability is an unknown functionality of the component SQLite Database. The manipulation leads to cleartext storage in a file or on disk. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229819.	2.3	More Detail
CVE-2023-33182	Contacts app for Nextcloud easily syncs contacts from various devices with your Nextcloud and allows editing. The unsanitized SVG is converted to a JavaScript blob (in memory data) that the Avatar can't render. Due to this constellation the missing sanitization does not seem to be exploitable. It is recommended that the Contacts app is upgraded to 5.0.3 or 4.2.4	0.0	More Detail
CVE-2022-32682	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32721	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32716	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2023-1601	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Detail
CVE-2023-1588	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-32717	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32718	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32719	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32720	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32722	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32723	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32724	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32725	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32673	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32726	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32727	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32728	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32729	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32672	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32714	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32715	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32731	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32702	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32703	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-32667	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32668	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32704	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32705	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32706	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32669	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32708	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32709	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32670	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32710	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32671	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32711	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32712	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32713	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32730	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32732	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32681	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32733	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-32694	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32693	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32691	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32690	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32689	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32688	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32677	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32687	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32686	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32678	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32679	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32685	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32684	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32683	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32701	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32680	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32695	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32696	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail

CVE Number	Description	Base Score	Refer
CVE-2018-8661	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2018. Notes: none.	N/A	More Detail
CVE-2022-24580	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-24580. Reason: This candidate is a duplicate of CVE-2023-24580. A typo caused the wrong ID to be used. Notes: All CVE users should reference CVE-2023-24580 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Detail
CVE-2022-32734	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32735	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-48138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-26829. Reason: This candidate is a reservation duplicate of CVE-2023-26829. Notes: All CVE users should reference CVE-2023-26829 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Detail
CVE-2022-48137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-26830. Reason: This candidate is a reservation duplicate of CVE-2023-26830. Notes: All CVE users should reference CVE-2023-26830 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Detail
CVE-2022-32736	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32737	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32738	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32674	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2023-2994	Rejected reason: This 2023 CVE was incorrectly assigned instead of a 2022 CVE.	N/A	More Detail
CVE-2022-32675	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32699	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32676	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2023-29079	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue in a customer-controlled product. Notes: none.	N/A	More Detail
CVE-2022-32698	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2023-29078	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue in a customer-controlled product. Notes: none.	N/A	More Detail
CVE-2022-32697	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail
CVE-2022-32700	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Detail