SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 November 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-2023-37924	Apache Software Foundation Apache Submarine has an SQL injection vulnerability when a user logs in. This issue can result in unauthorized login. Now we have fixed this issue and now user must have the correct login to access workbench. This issue affects Apache Submarine: from 0.7.0 before 0.8.0. We recommend that all submarine users with 0.7.0 upgrade to 0.8.0, which not only fixes the issue, supports the oidc authentication mode, but also removes the case of unauthenticated logins. If using the version lower than 0.8.0 and not want to upgrade, you can try cherry-pick PR https://github.com/apache/submarine/pull/1037 https://github.com/apache/submarine/pull/1054 and rebuild the submarine-server image to fix this.	9.8	More Details
CVE-2023-49046	Stack Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the devName parameter in the function formAddMacfilterRule.	9.8	More Details
CVE-2023-41999	An authentication bypass exists in Arcserve UDP prior to version 9.2. An unauthenticated, remote attacker can obtain a valid authentication identifier that allows them to authenticate to the management console and perform tasks that require authentication.	9.8	More Details
CVE-2023-42000	Arcserve UDP prior to 9.2 contains a path traversal vulnerability in com.ca.arcflash.ui.server.servlet.FileHandlingServlet.doUpload(). An unauthenticated remote attacker can exploit it to upload arbitrary files to any location on the file system where the UDP agent is installed.	9.8	More Details
CVE-2023-49040	An issue in Tneda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the adslPwd parameter in the form_fast_setting_internet_set function.	9.8	More Details
CVE-2023-49042	Heap Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the schedStartTime parameter or the schedEndTime parameter in the function setSchedWifi.	9.8	More Details
CVE-2023-4922	The WPB Show Core WordPress plugin through 2.2 is vulnerable to a local file inclusion via the `path` parameter.	9.8	More Details
CVE-2023-5604	The Asgaros Forum WordPress plugin before 2.7.1 allows forum administrators, who may not be WordPress (super-)administrators, to set insecure configuration that allows unauthenticated users to upload dangerous files (e.g. .php, .phtml), potentially leading to remote code execution.	9.8	More Details
CVE-2023-5974	The WPB Show Core WordPress plugin through 2.2 is vulnerable to server-side request forgery (SSRF) via the `path` parameter.	9.8	More Details
CVE-2023-6329	An authentication bypass vulnerability exists in Control iD iDSecure v4.7.32.0. The login routine used by iDS-Core.dll contains a "passwordCustom" option that allows an unauthenticated attacker to compute valid credentials that can be used to bypass authentication and act as an administrative user.	9.8	More Details
CVE-2023-49044	Stack Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the ssid parameter in the function form_fast_setting_wifi_set.	9.8	More Details
CVE-2023-46349	In the module "Product Catalog (CSV, Excel) Export/Update" (updateproducts) < 3.8.5 from MyPrestaModules for PrestaShop, a guest can perform SQL injection. The method `productsUpdateModel::getExportIds()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-46480	An issue in OwnCast v.0.1.1 allows a remote attacker to execute arbitrary code and obtain sensitive information via the authHost parameter of the indieauth function.	9.8	More Details
CVE-2023-48188	SQL injection vulnerability in PrestaShop opartdevis v.4.5.18 thru v.4.6.12 allows a remote attacker to execute arbitrary code via a crafted script to the getModuleTranslation function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47503	An issue in jflyfox jfinalCMS v.5.1.0 allows a remote attacker to execute arbitrary code via a crafted script to the login.jsp component in the template management module.	9.8	More Details
CVE-2023-3368	Command injection in `/main/webservices/additional_webservices.php` in Chamilo LMS <= v1.11.20 allows unauthenticated attackers to obtain remote code execution via improper neutralisation of special characters. This is a bypass of CVE-2023-34960.	9.8	More Details
CVE-2023-3533	Path traversal in file upload functionality in `/main/webservices/additional_webservices.php` in Chamilo LMS <= v1.11.20 allows unauthenticated attackers to perform stored cross-site scripting attacks and obtain remote code execution via arbitrary file write.	9.8	More Details
CVE-2023-3545	Improper sanitisation in `main/inc/lib/fileUpload.lib.php` in Chamilo LMS <= v1.11.20 on Windows and Apache installations allows unauthenticated attackers to bypass file upload security protections and obtain remote code execution via uploading of `.htaccess` file. This vulnerability may be exploited by privileged attackers or chained with unauthenticated arbitrary file write vulnerabilities, such as CVE-2023-3533, to achieve remote code execution.	9.8	More Details
CVE-2023-48022	Anyscale Ray 2.6.3 and 2.8.0 allows a remote attacker to execute arbitrary code via the job submission API. NOTE: the vendor's position is that this report is irrelevant because Ray, as stated in its documentation, is not intended for use outside of a strictly controlled network environment	9.8	More Details
CVE-2023-49313	A dylib injection vulnerability in XMachOViewer 0.04 allows attackers to compromise integrity. By exploiting this, unauthorized code can be injected into the product's processes, potentially leading to remote control and unauthorized access to sensitive user data.	9.8	More Details
CVE-2023-41264	Netwrix Usercube before 6.0.215, in certain misconfigured on-premises installations, allows authentication bypass on deployment endpoints, leading to privilege escalation. This only occurs if the configuration omits the required restSettings.AuthorizedClientId and restSettings.AuthorizedSecret fields (for the POST /api/Deployment/ExportConfiguration and POST /api/Deployment endpoints).	9.8	More Details
CVE-2023-5047	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in DRD Fleet Leasing DRDrive allows SQL Injection.This issue affects DRDrive: before 20231006.	9.8	More Details
CVE-2023-41998	Arcserve UDP prior to 9.2 contained a vulnerability in the com.ca.arcflash.rps.webservice.RPSService4CPMImpl interface. A routine exists that allows an attacker to upload and execute arbitrary files.	9.8	More Details
CVE-2023-49043	Buffer Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the wpapsk_crypto parameter in the function fromSetWirelessRepeat.	9.8	More Details
CVE-2023-29076	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	9.8	More Details
CVE-2023-2889	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Veon Computer Service Tracking Software allows SQL Injection.This issue affects Service Tracking Software: before crm 2.0.	9.8	More Details
CVE-2023-2437	The UserPro plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.1.1. This is due to insufficient verification on the user being supplied during a Facebook login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email. An attacker can leverage CVE-2023-2448 and CVE-2023-2446 to get the user's email address to successfully exploit this vulnerability.	9.8	More Details
CVE-2023-2449	The UserPro plugin for WordPress is vulnerable to unauthorized password resets in versions up to, and including 5.1.1. This is due to the plugin using native password reset functionality, with insufficient validation on the password reset function (userpro_process_form). The function uses the plaintext value of a password reset key instead of a hashed value which means it can easily be retrieved and subsequently used. An attacker can leverage CVE-2023-2448 and CVE-2023-2446, or another vulnerability like SQL Injection in another plugin or theme installed on the site to successfully exploit this vulnerability.	9.8	More Details
CVE-2023-45377	In the module "Chronopost Official" (chronopost) for PrestaShop, a guest can perform SQL injection. The script PHP `cancelSkybill.php` own a sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-46357	In the module "Cross Selling in Modal Cart" (motivationsale) < 3.5.0 from MyPrestaModules for PrestaShop, a guest can perform SQL injection. The method `motivationsaleDataModel::getProductsByIds()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-29073	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	9.8	More Details
CVE-2023-29074	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	9.8	More Details
CVE-2023-29075	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	9.8	More Details
CVE-2023-48193	Insecure Permissions vulnerability in JumpServer GPLv3 v.3.8.0 allows a remote attacker to execute arbitrary code via bypassing the command filtering function. NOTE: this is disputed because command filtering is not intended to restrict what code can be run by authorized users who are allowed to execute files.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3377	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Veribilim Software Computer Veribase allows SQL Injection.This issue affects Veribase: through 20231123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-3631	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Medart Health Services Medart Notification Panel allows SQL Injection.This issue affects Medart Notification Panel: through 20231123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-49208	scheme/webauthn.c in Glewlwyd SSO server before 2.7.6 has a possible buffer overflow during FIDO2 credentials validation in webauthn registration.	9.8	More Details
CVE-2023-49210	The openssl (aka node-openssl) NPM package through 2.0.0 was characterized as "a nonsense wrapper with no real purpose" by its author, and accepts an opts argument that contains a verb field (used for command execution). NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2023-49214	Usedesk before 1.7.57 allows chat template injection.	9.8	More Details
CVE-2023-46575	A SQL injection vulnerability exists in Meshery prior to version v0.6.179, enabling a remote attacker to retrieve sensitive information and execute arbitrary code through the “order” parameter	9.8	More Details
CVE-2023-48312	capsule-proxy is a reverse proxy for the capsule operator project. Affected versions are subject to a privilege escalation vulnerability which is based on a missing check if the user is authenticated based on the `TokenReview` result. All the clusters running with the `anonymous-auth` Kubernetes API Server setting disable (set to `false`) are affected since it would be possible to bypass the token review mechanism, interacting with the upper Kubernetes API Server. This privilege escalation cannot be exploited if you're relying only on client certificates (SSL/TLS). This vulnerability has been addressed in version 0.4.6. Users are advised to upgrade.	9.8	More Details
CVE-2023-49312	Precision Bridge PrecisionBridge.exe (aka the thick client) before 7.3.21 allows an integrity violation in which the same license key is used on multiple systems, via vectors involving a Process Hacker memory dump, error message inspection, and modification of a MAC address.	9.1	More Details
CVE-2023-41807	Improper Privilege Management vulnerability in Pandora FMS on all allows Privilege Escalation. This vulnerability allows a user to escalate permissions on the system shell. This issue affects Pandora FMS: from 700 through 773.	9.1	More Details
CVE-2023-5559	The 10Web Booster WordPress plugin before 2.24.18 does not validate the option name given to some AJAX actions, allowing unauthenticated users to delete arbitrary options from the database, leading to denial of service.	9.1	More Details
CVE-2023-48023	Anyscale Ray 2.6.3 and 2.8.0 allows /log_proxy SSRF. NOTE: the vendor's position is that this report is irrelevant because Ray, as stated in its documentation, is not intended for use outside of a strictly controlled network environment	9.1	More Details
CVE-2023-28812	There is a buffer overflow vulnerability in a web browser plug-in could allow an attacker to exploit the vulnerability by sending crafted messages to computers installed with this plug-in, which could lead to arbitrary code execution or cause process exception of the plug-in.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2023-2497	The UserPro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.1.0. This is due to missing or incorrect nonce validation on the 'import_settings' function. This makes it possible for unauthenticated attackers to exploit PHP Object Injection due to the use of unserialize() on the user supplied parameter via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2023-29770	In Sentrifugo 3.5, the AssetsController::uploadsaveAction function allows an authenticated attacker to upload any file without extension filtering.
CVE-2023-47781	Cross-Site Request Forgery (CSRF) vulnerability in Thrive Themes Thrive Theme Builder < 3.24.2 versions.
CVE-2023-49213	The API endpoints in Ironman PowerShell Universal 3.0.0 through 4.2.0 allow remote attackers to execute arbitrary commands via crafted HTTP requests if a param block is used, due to invalid sanitization of input strings. The fixed versions are 3.10.2, 4.1.10, and 4.2.1.
CVE-2023-48106	Buffer Overflow vulnerability in zlib-ng minizip-ng v.4.0.2 allows an attacker to execute arbitrary code via a crafted file to the mz_path_resolve function in the mz_os.c file.
CVE-2023-47350	Cross-Site Request Forgery (CSRF) vulnerability in SwiftyEdit Content Management System prior to v1.2.0, allows remote attackers to escalate privileges via the user password update functionality.
CVE-2023-31275	An uninitialized pointer use vulnerability exists in the functionality of WPS Office 11.2.0.11537 that handles Data elements in an Excel file. A specially crafted malformed file can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability.

CVE Number	Description
CVE-2023-32616	A use-after-free vulnerability exists in the way Foxit Reader 12.1.2.15356 handles 3D annotations. A specially crafted Javascript code inside a malicious PDF documen can trigger reuse of a previously freed object, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.
CVE-2023-35985	An arbitrary file creation vulnerability exists in the Javascript exportDataObject API of Foxit Reader 12.1.3.15356 due to a failure to properly validate a dangerous extension. A specially crafted malicious file can create files at arbitrary locations, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted malicious site if the browser plugin extension is enabled.
CVE-2023-38573	A use-after-free vulnerability exists in the way Foxit Reader 12.1.2.15356 handles a signature field. A specially crafted Javascript code inside a malicious PDF documer can trigger reuse of a previously freed object, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.
CVE-2023-39542	A code execution vulnerability exists in the Javascript saveAs API of Foxit Reader 12.1.3.15356. A specially crafted malformed file can create arbitrary files, which can lead to remote code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.
CVE-2023-40194	An arbitrary file creation vulnerability exists in the Javascript exportDataObject API of Foxit Reader 12.1.3.15356 due to mistreatment of whitespace characters. A specially crafted malicious file can create files at arbitrary locations, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.
CVE-2023-41257	A type confusion vulnerability exists in the way Foxit Reader 12.1.2.15356 handles field value properties. A specially crafted Javascript code inside a malicious PDF document can trigger this vulnerability, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.
CVE-2023-48107	Buffer Overflow vulnerability in zlib-ng minizip-ng v.4.0.2 allows an attacker to execute arbitrary code via a crafted file to the mz_path_has_slash function in the mz_os.c file.
CVE-2023-47250	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, broken Access Control on X11 server sockets allows authenticated attackers (with access to a VNC session) to access the X11 desktops of other users by specifying their DISPLAY ID. This allows complete control of their desktop, including the ability to inject keystrokes and perform a keylogging attack.
CVE-2023-49102	NZBGet 21.1 allows authenticated remote code execution because the unarchive programs (7za and unrar) preserve executable file permissions. An attacker with the Control capability can execute a file by setting the value of SevenZipCommand or UnrarCmd. NOTE: This vulnerability only affects products that are no longer supporte by the maintainer.
CVE-2023-5466	The Wp anything slider plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.1 due to insufficient escaping o the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2023-4223	Unrestricted file upload in `/main/inc/ajax/document.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code execution via uploading of PHP files.
CVE-2023-4224	Unrestricted file upload in `/main/inc/ajax/dropbox.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code execution via uploading of PHP files.
CVE-2023-4225	Unrestricted file upload in `/main/inc/ajax/exercise.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code execution via uploading of PHP files.
CVE-2023-4226	Unrestricted file upload in `/main/inc/ajax/work.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code execution via uploading of PHP files.
CVE-2023-6009	The UserPro plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.1.4 due to insufficient restriction on the 'userpro_update_user_profile' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wp_capabilities' parameter during a profile update.
CVE-2023-6201	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Univera Computer System Panorama allows Comman Injection.This issue affects Panorama: before 8.0.
CVE-2023-47315	Headwind MDM Web panel 5.22.1 is vulnerable to Incorrect Access Control due to a hard-coded JWT Secret. The secret is hardcoded into the source code available to anyone on Git Hub. This secret is used to sign the application’s JWT token and verify the incoming user-supplied tokens.
CVE-2023-5465	The Popup with fancybox plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

CVE Number	Description
CVE-2022-41678	Once an user is authenticated on Jolokia, he can potentially trigger arbitrary code execution. In details, in ActiveMQ configurations, jetty allows org.jolokia.http.AgentServlet to handler request to /api/jolokia org.jolokia.http.HttpRequestHandler#handlePostRequest is able to create JmxRequest through JSONObject. And calls to org.jolokia.http.HttpRequestHandler#executeRequest. Into deeper calling stacks, org.jolokia.handler.ExecHandler#doHandleRequest can be invoked through refection. This could lead to RCE through via various mbeans. One example is unrestricted deserialization in jdk.management.jfr.FlightRecorderMXBeanImpl which exists on Java version above 11. 1 Call newRecording. 2 Call setConfiguration. And a webshell data hides in it. 3 Call startRecording. 4 Call copyTo method. The webshell will be written to a .jsp file. The mitigation is to restrict (by default) the actions authorized on Jolokia, or disable Jolokia. A more restrictive Jolokia configuration has been defined in default ActiveMQ distribution. We encourage users to upgrade to ActiveMQ distributions version including updated Jolokia configuration: 5.16.6, 5.17.4, 5.18.0, 6.0.0.
CVE-2023-2440	The UserPro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.1.1. This is due to missing nonce validation in the 'admin_page', 'userpro_verify_user' and 'verifyUnverifyAllUsers' functions. This makes it possible for unauthenticated attackers to modify the role of verified users to elevate verified user privileges to that of any user such as 'administrator' via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2023-43082	Dell Unity prior to 5.3 contains a 'man in the middle' vulnerability in the vmadapter component. If a customer has a certificate signed by a third-party public Certificate Authority, the vCenter CA could be spoofed by an attacker who can obtain a CA-signed certificate.
CVE-2023-41808	Improper Privilege Management vulnerability in Pandora FMS on all allows Privilege Escalation. This vulnerability allows an unauthorised user to escalate and read sensitive files as if they were root. This issue affects Pandora FMS: from 700 through 773.
CVE-2022-41951	OroPlatform is a PHP Business Application Platform (BAP) designed to make development of custom business applications easier and faster. Path Traversal is possibl in `Oro\Bundle\GaufretteBundle\FileManager::getTemporaryFileName`. With this method, an attacker can pass the path to a non-existent file, which will allow writing th content to a new file that will be available during script execution. This vulnerability has been fixed in version 5.0.9.
CVE-2023-41791	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed users with low privileges to introduce Javascript executables via a translation string that could affect the integrity of some configuration files. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-5607	An improper limitation of a path name to a restricted directory (path traversal) vulnerability in the TACC ePO extension, for on-premises ePO servers, prior to version 8.4.0 could lead to an authorised administrator attacker executing arbitrary code through uploading a specially crafted GTI reputation file. The attacker would need the appropriate privileges to access the relevant section of the User Interface. The import logic has been updated to restrict file types and content.
CVE-2023-49075	The Admin Classic Bundle provides a Backend UI for Pimcore. `AdminBundle\Security\PimcoreUserTwoFactorCondition` introduced in v11 disable the two factor authentication for all non-admin security firewalls. An authenticated user can access the system without having to provide the two factor credentials. This issue has bee patched in version 1.2.2.
CVE-2023-6263	An issue was discovered by IPVM team in Network Optix NxCloud before 23.1.0.40440. It was possible to add a fake VMS server to NxCloud by using the exact identification of a legitimate VMS server. As result, it was possible to retrieve authorization headers from legitimate users when the legitimate client connects to th fake VMS server.
CVE-2023-41806	Improper Privilege Management vulnerability in Pandora FMS on all allows Privilege Escalation. This vulnerability causes that a bad privilege assignment could cause a DOS attack that affects the availability of the Pandora FMS server. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-45539	HAProxy before 2.8.2 accepts # as part of the URI component, which might allow remote attackers to obtain sensitive information or have unspecified other impact upo misinterpretation of a path_end rule, such as routing index.html#.png to a static server.
CVE-2023-28813	An attacker could exploit a vulnerability by sending crafted messages to computers installed with this plug-in to modify plug-in parameters, which could cause affected computers to download malicious files.
CVE-2023-6254	A Vulnerability in OTRS AgentInterface and ExternalInterface allows the reading of plain text passwords which are send back to the client in the server response- This issue affects OTRS: from 8.0.X through 8.0.37.
CVE-2023-43887	Libde265 v1.0.12 was discovered to contain multiple buffer overflows via the num_tile_columns and num_tile_row parameters in the function pic_parameter_set::dump
CVE-2023-4220	Unrestricted file upload in big file upload functionality in `/main/inc/lib/javascript/bigupload/inc/bigUpload.php` in Chamilo LMS <= v1.11.24 allows unauthenticated attackers to perform stored cross-site scripting attacks and obtain remote code execution via uploading of web shell.
CVE-2023-4667	The web interface of the PAC Device allows the device administrator user profile to store malicious scripts in some fields. The stored malicious script is then executed when the GUI is opened by any users of the webserver administration interface. The root cause of the vulnerability is inadequate input validation and output encoding i the web administration interface component of the firmware. This could lead to unauthorized access and data leakage
CVE-2023-5822	The Drag and Drop Multiple File Upload - Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads to insufficient file type validation in the 'dnd_upload_cf7_upload' function in versions up to, and including, 1.3.7.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This can be exploited if a user authorized to edit form, which means editor privileges or above, has adde a 'multiple file upload' form field with '*' acceptable file types.

CVE Number	Description
CVE-2023-5815	The News & Blog Designer Pack – WordPress Blog Plugin — (Blog Post Grid, Blog Post Slider, Blog Post Carousel, Blog Post Ticker, Blog Post Masonry) plugin for WordPress is vulnerable to Remote Code Execution via Local File Inclusion in all versions up to, and including, 3.4.1 via the bdp_get_more_post function hooked via a nopriv AJAX. This is due to function utilizing an unsafe extract() method to extract values from the POST variable and passing that input to the include() function. This makes it possible for unauthenticated attackers to include arbitrary PHP files and achieve remote code execution. On vulnerable Docker configurations it may be possible for an attacker to create a PHP file and then subsequently include it to achieve RCE.
CVE-2023-42004	IBM Security Guardium 11.3, 11.4, and 11.5 is potentially vulnerable to CSV injection. A remote attacker could execute malicious commands due to improper validation of csv file contents. IBM X-Force ID: 265262.
CVE-2023-40056	SQL Injection Remote Code Vulnerability was found in the SolarWinds Platform. This vulnerability can be exploited with a low privileged account.
CVE-2023-3103	Authentication bypass vulnerability, the exploitation of which could allow a local attacker to perform a Man-in-the-Middle (MITM) attack on the robot's camera video stream. In addition, if a MITM attack is carried out, it is possible to consume the robot's resources, which could lead to a denial-of-service (DOS) condition.
CVE-2023-49145	Apache NiFi 0.7.0 through 1.23.2 include the JoltTransformJSON Processor, which provides an advanced configuration user interface that is vulnerable to DOM-based cross-site scripting. If an authenticated user, who is authorized to configure a JoltTransformJSON Processor, visits a crafted URL, then arbitrary JavaScript code can be executed within the session context of the authenticated user. Upgrading to Apache NiFi 1.24.0 or 2.0.0-M1 is the recommended mitigation.
CVE-2023-41139	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.
CVE-2023-41140	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
CVE-2023-49314	Asana Desktop 2.1.0 on macOS allows code injection because of specific Electron Fuses. There is inadequate protection against code injection through settings such as RunAsNode and EnableNodeCliInspectArguments, and thus r3ggi/electroniz3r can be used to perform an attack.
CVE-2023-46944	An issue in GitKraken GitLens before v.14.0.0 allows an attacker to execute arbitrary code via a crafted file to the Visual Studio Codes workspace trust component.
CVE-2023-35127	Stack-based buffer overflow may occur when Fuji Electric Tellus Lite V-Simulator parses a specially-crafted input file.
CVE-2023-40152	When Fuji Electric Tellus Lite V-Simulator parses a specially-crafted input file an out of bounds write may occur.
CVE-2023-46814	A binary hijacking vulnerability exists within the VideoLAN VLC media player before 3.0.19 on Windows. The uninstaller attempts to execute code with elevated privileges out of a standard user writable location. Standard users may use this to gain arbitrary code execution as SYSTEM.
CVE-2023-29069	A maliciously crafted DLL file can be forced to install onto a non-default location, and attacker can overwrite parts of the product with malicious DLLs. These files may then have elevated privileges leading to a Privilege Escalation vulnerability.
CVE-2023-6157	Improper neutralization of livestatus command delimiters in ajax_search in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users.
CVE-2023-41789	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allows an attacker to perform cookie hijacking and log in as that user without the need for credentials. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-41788	Unrestricted Upload of File with Dangerous Type vulnerability in Pandora FMS on all allows Accessing Functionality Not Properly Constrained by ACLs. This vulnerability allows attackers to execute code via PHP file uploads. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-6156	Improper neutralization of livestatus command delimiters in the availability timeline in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users.
CVE-2023-41790	Uncontrolled Search Path Element vulnerability in Pandora FMS on all allows Leveraging/Manipulating Configuration File Search Paths. This vulnerability allows to access the server configuration file and to compromise the database. This issue affects Pandora FMS: from 700 through 773.

CVE Number	Description
CVE-2023-49322	Certain WithSecure products allow a Denial of Service because there is an unpack handler crash that can lead to a scanning engine crash. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Clier Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, WithSecure Linux Security 64 12.0, WithSecure Linux Protection 12.0, and WithSecure Atlant 1.0.35-1.
CVE-2023-5906	The Job Manager & Career WordPress plugin before 1.4.4 contains a vulnerability in the Directory Listings system, which allows an unauthorized user to view and download private files of other users. This vulnerability poses a serious security threat because it allows an attacker to gain access to confidential data and files of othe users without their permission.
CVE-2023-5239	The Security & Malware scan by CleanTalk WordPress plugin before 2.121 retrieves client IP addresses from potentially untrusted headers, allowing an attacker to manipulate its value. This may be used to bypass bruteforce protection.
CVE-2023-49047	Tenda AX1803 v1.0.0.1 contains a stack overflow via the devName parameter in the function formSetDeviceName.
CVE-2023-5983	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Botanik Software Pharmacy Automation allows Retrieve Embedded Sensitive Data.This issue affects Pharmacy Automation: before 2.1.133.0.
CVE-2023-49068	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache DolphinScheduler.This issue affects Apache DolphinScheduler: before 3.2.1. Users are recommended to upgrade to version 3.2.1, which fixes the issue. At the time of disclosure of this advisory, this version has not yet been released. In the mean time, we recommend you make sure the logs are only available to trusted operators.
CVE-2023-49298	OpenZFS through 2.1.13 and 2.2.x through 2.2.1, in certain scenarios involving applications that try to rely on efficient copying of file data, can replace file contents with zero-valued bytes and thus potentially disable security mechanisms. NOTE: this issue is not always security related, but can be security related in realistic situations. A possible example is cp, from a recent GNU Core Utilities (coreutils) version, when attempting to preserve a rule set for denying unauthorized access. (One might use cp when configuring access control, such as with the /etc/hosts.deny file specified in the IBM Support reference.) NOTE: this issue occurs less often in version 2.2.1, and i versions before 2.1.4, because of the default configuration in those versions.
CVE-2023-4595	An information exposure vulnerability has been found, the exploitation of which could allow a remote user to retrieve sensitive information stored on the server such as credential files, configuration files, application files, etc., simply by appending any of the following parameters to the end of the URL: %00 %0a, %20, %2a, %a0, %aa, %c0 and %ca.
CVE-2023-6252	Path traversal vulnerability in Chalemelon Power framework, affecting the getImage parameter. This vulnerability could allow a remote user to read files located on the server and gain access to sensitive information such as configuration files.
CVE-2023-48796	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache DolphinScheduler. The information exposed to unauthorized actors may include sensitive data such as database credentials. Users who can't upgrade to the fixed version can also set environment variable `MANAGEMENT_ENDPOINTS_WEB_EXPOSURE_INCLUDE=health,metrics,prometheus` to workaround this, or add the following section in the `application.yaml` file ``` management: endpoints: web: exposure: include: health,metrics,prometheus ``` This issue affects Apache DolphinScheduler: from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2, which fixes the issue.
CVE-2023-44303	RVTools, Version 3.9.2 and above, contain a sensitive data exposure vulnerability in the password encryption utility (RVToolsPasswordEncryption.exe) and main application (RVTools.exe). A remote unauthenticated attacker with access to stored encrypted passwords from a users' system could potentially exploit this vulnerability leading to the disclosure of encrypted passwords in clear text. This vulnerability is caused by an incomplete fix for CVE-2020-27688.
CVE-2022-44010	An issue was discovered in ClickHouse before 22.9.1.2603. An attacker could send a crafted HTTP request to the HTTP Endpoint (usually listening on port 8123 by default), causing a heap-based buffer overflow that crashes the process. This does not require authentication. The fixed versions are 22.9.1.2603, 22.8.2.11, 22.7.4.16, 22.6.6.16, and 22.3.12.19.
CVE-2023-49316	In Math/BinaryField.php in phpseclib 3 before 3.0.34, excessively large degrees can lead to a denial of service.
CVE-2023-49030	SQL Injection vulnerability in32ns KLive v.2019-1-19 and before allows a remote attacker to obtain sensitive information via a crafted script to the web/user.php component.
CVE-2023-47016	radare2 5.8.9 has an out-of-bounds read in r_bin_object_set_items in libr/bin/bobj.c, causing a crash in r_read_le32 in libr/include/r_endian.h.
CVE-2023-30581	The use of __proto__ in process.mainModule.__proto__.require() can bypass the policy mechanism and require modules outside of the policy.json definition. This vulnerability affects all users using the experimental policy mechanism in all active release lines: v16, v18 and, v20. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js
CVE-2023-30590	The generateKeys() API function returned from crypto.createDiffieHellman() only generates missing (or outdated) keys, that is, it only generates a private key if none ha been set yet, but the function is also needed to compute the corresponding public key after calling setPrivateKey(). However, the documentation says this API call: "Generates private and public Diffie-Hellman key values". The documented behavior is very different from the actual behavior, and this difference could easily lead to security issues in applications that use these APIs as the DiffieHellman may be used as the basis for application-level security, implications are consequently broad.
CVE-2023-48848	An arbitrary file read vulnerability in ureport v2.2.9 allows a remote attacker to arbitrarily read files on the server by inserting a crafted path.

CVE Number	Description
CVE-2023-49062	Katran could disclose non-initialized kernel memory as part of an IP header. The issue was present for IPv4 encapsulation and ICMP (v4) Too Big packet generation. After a bpf_xdp_adjust_head call, Katran code didn't initialize the Identification field for the IPv4 header, resulting in writing content of kernel memory in that field of IP header. The issue affected all Katran versions prior to commit 6a03106ac1eab39d0303662963589ecb2374c97f
CVE-2023-46589	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.1.15, from 9.0.0-M1 through 9.0.82 and from 8.5.0 through 8.5.95 did not correctly parse HTTP trailer headers. A trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Users are recommended to upgrade to version 11.0.0-M11 onwards, 10.1.16 onwards, 9.0.83 onwards or 8.5.96 onwards, which fix the issue.
CVE-2023-6151	Incorrect Use of Privileged APIs vulnerability in ESKOM Computer e-municipality module allows Collect Data as Provided by Users.This issue affects e-municipality module: before v.105.
CVE-2023-6150	Incorrect Use of Privileged APIs vulnerability in ESKOM Computer e-municipality module allows Collect Data as Provided by Users.This issue affects e-municipality module: before v.105.
CVE-2023-30585	A vulnerability has been identified in the Node.js (.msi version) installation process, specifically affecting Windows users who install Node.js using the .msi installer. This vulnerability emerges during the repair operation, where the "msiexec.exe" process, running under the NT AUTHORITY\SYSTEM context, attempts to read the %USERPROFILE% environment variable from the current user's registry. The issue arises when the path referenced by the %USERPROFILE% environment variable does not exist. In such cases, the "msiexec.exe" process attempts to create the specified path in an unsafe manner, potentially leading to the creation of arbitrary folder in arbitrary locations. The severity of this vulnerability is heightened by the fact that the %USERPROFILE% environment variable in the Windows registry can be modified by standard (or "non-privileged") users. Consequently, unprivileged actors, including malicious entities or trojans, can manipulate the environment variable key to deceive the privileged "msiexec.exe" process. This manipulation can result in the creation of folders in unintended and potentially malicious locations. It is important to note that this vulnerability is specific to Windows users who install Node.js using the .msi installer. Users who opt for other installation methods are not affected by this particular issue.
CVE-2023-48105	An heap overflow vulnerability was discovered in Bytecode alliance wasm-micro-runtime v.1.2.3 allows a remote attacker to cause a denial of service via the wasm_loader_prepare_bytecode function in core/iwasm/interpreter/wasm_loader.c.
CVE-2023-4398	An integer overflow vulnerability in the source code of the QuickSec IPSec toolkit used in the VPN feature of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions on an affected device by sending a crafted IKE packet.
CVE-2023-6118	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1.
CVE-2023-28811	There is a buffer overflow in the password recovery feature of Hikvision NVR/DVR models. If exploited, an attacker on the same local area network (LAN) could cause the device to malfunction by sending specially crafted packets to an unpatched device.
CVE-2023-44290	Dell Command | Monitor versions prior to 10.10.0, contain an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability while repairing/changing installation, leading to privilege escalation.
CVE-2023-6007	The UserPro plugin for WordPress is vulnerable to unauthorized access of data, modification of data, loss of data due to a missing capability check on multiple function in all versions up to, and including, 5.1.1. This makes it possible for unauthenticated attackers to add, modify, or delete user meta and plugin options.
CVE-2023-39253	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system.
CVE-2023-5299	A user with a standard account in Fuji Electric Tellus Lite may overwrite files in the system.
CVE-2023-4590	Buffer overflow vulnerability in Frhed hex editor, affecting version 1.6.0. This vulnerability could allow an attacker to execute arbitrary code via a long filename argumen through the Structured Exception Handler (SEH) registers.
CVE-2023-44289	Dell Command | Configure versions prior to 4.11.0, contain an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability while repairing/changing installation, leading to privilege escalation.
CVE-2023-43086	Dell Command | Configure, versions prior to 4.11.0, contains an improper access control vulnerability. A local malicious user could potentially modify files inside installation folder during application upgrade, leading to privilege escalation.
CVE-2023-48646	Zoho ManageEngine RecoveryManager Plus before 6070 allows admin users to execute arbitrary commands via proxy settings.

CVE Number	Description
CVE-2023-2841	The Advanced Local Pickup for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the id parameter in versions up to, and including, 1.5.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with admin-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2023-6219	The BookingPress plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file validation on the 'bookingpress_process_upload' function in version up to, and including, 1.0.76. This makes it possible for authenticated attackers with administrator-level capabilities or above, to upload arbitrary files on the affected site server which may make remote code execution possible.
CVE-2023-27451	Server-Side Request Forgery (SSRF) vulnerability in Darren Cooney Instant Images plugin <= 5.1.0.2 versions.
CVE-2023-4222	Command injection in `main/lp/openoffice_text_document.class.php` in Chamilo LMS <= v1.11.24 allows users permitted to upload Learning Paths to obtain remote code execution via improper neutralisation of special characters.
CVE-2023-6304	A vulnerability was found in Tecno 4G Portable WiFi TR118 TR118-M30E-RR-D-EnFrArSwHaPo-OP-V008-20220830. It has been declared as critical. This vulnerability affects unknown code of the file /goform/goform_get_cmd_process of the component Ping Tool. The manipulation of the argument url leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-246130 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-4221	Command injection in `main/lp/openoffice_presentation.class.php` in Chamilo LMS <= v1.11.24 allows users permitted to upload Learning Paths to obtain remote code execution via improper neutralisation of special characters.
CVE-2023-47766	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timo Reith Post Status Notifier Lite plugin <= 1.11.0 versions.
CVE-2023-47768	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson Footer Putter plugin <= 1.17 versions.
CVE-2023-47773	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YAS Global Team Permalinks Customizer plugin <= 2.8.2 versions
CVE-2023-48161	Buffer Overflow vulnerability in GifLib Project GifLib v.5.2.1 allows a local attacker to obtain sensitive information via the DumpSCreen2RGB function in gif2rgb.c
CVE-2023-47790	Cross-Site Request Forgery (CSRF) leading to Cross-Site Scripting (XSS) vulnerability in Poporon Pz-LinkCard plugin <= 2.4.8 versions.
CVE-2023-47785	Cross-Site Request Forgery (CSRF) vulnerability in LayerSlider plugin <= 7.7.9 versions.
CVE-2023-5921	Improper Enforcement of Behavioral Workflow vulnerability in DECE Software Geodi allows Functionality Bypass.This issue affects Geodi: before 8.0.0.27396.
CVE-2023-6293	Prototype Pollution in GitHub repository robinbuschmann/sequelize-typescript prior to 2.1.6.
CVE-2023-30496	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MagePeople Team WpBusTicketly plugin <= 5.2.5 versions.
CVE-2023-48712	Warpgate is an open source SSH, HTTPS and MySQL bastion host for Linux. In affected versions there is a privilege escalation vulnerability through a non-admin user account. Limited users can impersonate another user's account if only single-factor authentication is configured. If a user knows an admin username, opens the login screen and attempts to authenticate with an incorrect password they can subsequently enter a valid non-admin username and password they will be logged in as the admin user. All installations prior to version 0.9.0 are affected. All users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2023-48705	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application All users of Nautobot versions earlier than 1.6.6 or 2.0.5 are potentially affected by a cross-site scripting vulnerability. Due to incorrect usage of Django's `mark_safe()` API when rendering certain types of user-authored content; including custom links, job buttons, and computed fields; it is possible that users with permission to create or edit these types of content could craft a malicious payload (such as JavaScript code) that would be executed when rendering pages containing this content. The maintainers have fixed the incorrect uses of `mark_safe()` (generally by replacing them with appropriate use of `format_html()` instead) to prevent such malicious data from being executed. Users on Nautobot 1.6.x LTM should upgrade to v1.6.6 and users on Nautobot 2.0.x should upgrade to v2.0.5. Appropriate object permissions can and should be applied to restrict which users are permitte to create or edit the aforementioned types of user-authored content. Other than that, there is no direct workaround available.
CVE-2023-47767	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fla-shop.Com Interactive World Map plugin <= 3.2.0 versions.

CVE Number	Description
CVE-2023-4677	Cron log backup files contain administrator session IDs. It is trivial for any attacker who can reach the Pandora FMS Console to scrape the cron logs directory for cron log backups. The contents of these log files can then be abused to authenticate to the application as an administrator. This issue affects Pandora FMS <= 772.
CVE-2021-37942	A local privilege escalation issue was found with the APM Java agent, where a user on the system could attach a malicious plugin to an application running the APM Java agent. By using this vulnerability, an attacker could execute code at a potentially higher level of permissions than their user typically has access to.
CVE-2023-5972	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the Linux kernel. This issue could allow a local user to crash the system or escalat their privileges on the system.
CVE-2023-24023	Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in Bluetooth Core Specification 4.2 through 5.4 allow certain man-in-the-middle attacks that force a short key length, and might lead to discovery of the encryption key and live injection, aka BLUFFS.
CVE-2023-41786	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pandora FMS on all allows File Discovery. This vulnerability allows users with low privileges to download database backups. This issue affects Pandora FMS: from 700 through 772.
CVE-2021-22150	It was discovered that a user with Fleet admin permissions could upload a malicious package. Due to using an older version of the js-yaml library, this package would b loaded in an insecure manner, allowing an attacker to execute commands on the Kibana server.
CVE-2021-22142	Kibana contains an embedded version of the Chromium browser that the Reporting feature uses to generate the downloadable reports. If a user with permissions to generate reports is able to render arbitrary HTML with this browser, they may be able to leverage known Chromium vulnerabilities to conduct further attacks. Kibana contains a number of protections to prevent this browser from rendering arbitrary content.
CVE-2023-47821	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jannis Thuemmig Email Encoder plugin <= 2.1.8 versions.
CVE-2023-47467	Directory Traversal vulnerability in jeecg-boot v.3.6.0 allows a remote privileged attacker to obtain sensitive information via the file directory structure.
CVE-2023-47811	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Suresh KUMAR Mukhiya Anywhere Flash Embed plugin <= 1.0.5 versions.
CVE-2023-47812	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bamboo Mcr Bamboo Columns plugin <= 1.6.1 versions.
CVE-2023-47813	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in grandslambert Better RSS Widget plugin <= 2.8.1 versions.
CVE-2023-47814	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Waterloo Plugins BMI Calculator Plugin plugin <= 1.0.3 versions.
CVE-2023-47815	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Venutius BP Profile Shortcodes Extra plugin <= 2.5.2 versions.
CVE-2023-47816	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Charitable Donations & Fundraising Team Donation Forms by Charitable plugin <= 1.7.0.13 versions.
CVE-2023-47817	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mmrs151 Daily Prayer Time plugin <= 2023.10.13 versions.
CVE-2023-46673	It was identified that malformed scripts used in the script processor of an Ingest Pipeline could cause an Elasticsearch node to crash when calling the Simulate Pipeline API.
CVE-2022-44011	An issue was discovered in ClickHouse before 22.9.1.2603. An authenticated user (with the ability to load data) could cause a heap buffer overflow and crash the serve by inserting a malformed CapnProto object. The fixed versions are 22.9.1.2603, 22.8.2.11, 22.7.4.16, 22.6.6.16, and 22.3.12.19.
CVE-2023-47831	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in assorted[chips] DrawIt (draw.Io) plugin <= 1.1.3 versions.

CVE Number	Description
CVE-2023-33706	SysAid before 23.2.15 allows Indirect Object Reference (IDOR) attacks to read ticket data via a modified sid parameter to EmailHtmlSourceIframe.jsp or a modified srID parameter to ShowMessage.jsp.
CVE-2023-47312	Headwind MDM Web panel 5.22.1 is vulnerable to Incorrect Access Control due to Login Credential Leakage via Audit Entries.
CVE-2023-47839	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode eCommerce Product Catalog Plugin for WordPress plugin <= 3.3.26 versions.
CVE-2023-47835	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ARI Soft ARI Stream Quiz – WordPress Quizzes Builder plugin <= 1.2.32 versions.
CVE-2023-40002	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pluggabl LLC Booster for WooCommerce plugin <= 7.1.1 versions.
CVE-2023-47834	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExpressTech Quiz And Survey Master plugin <= 8.1.13 versions.
CVE-2023-47810	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Asdqwe Dev Ajax Domain Checker plugin <= 1.3.0 versions.
CVE-2023-47251	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, a Directory Traversal in the print function of the VNC service allows authenticated attackers (with access to a VNC session) to automatically transfer malicious PDF documents by moving them into the .spool directory, and then sending a signal to the VNC service, which automatically transfers them to the connected VNC client's filesystem.
CVE-2023-6265	** UNSUPPORTED WHEN ASSIGNED ** Draytek Vigor2960 v1.5.1.4 and v1.5.1.5 are vulnerable to directory traversal via the mainfunction.cgi dumpSyslog 'option' parameter allowing an authenticated attacker with access to the web management interface to delete arbitrary files. Vigor2960 is no longer supported.
CVE-2023-5386	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_delete_posts function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete arbitrary posts, including administrator posts, and posts not related to the Funnelforms Free plugin.
CVE-2023-2448	The UserPro plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'userpro_shortcode_template' function in versions up to, and including, 5.1.4. This makes it possible for unauthenticated attackers to arbitrary shortcode execution. An attacker can leverage CVE-2023-2446 to get sensitive information via shortcode.
CVE-2023-2446	The UserPro plugin for WordPress is vulnerable to sensitive information disclosure via the 'userpro' shortcode in versions up to, and including 5.1.1. This is due to insufficient restriction on sensitive user meta values that can be called via that shortcode. This makes it possible for authenticated attackers, with subscriber-level permissions, and above to retrieve sensitive user meta that can be used to gain access to a high privileged user account.
CVE-2023-4593	Path traversal vulnerability whose exploitation could allow an authenticated remote user to bypass SecurityManager's intended restrictions and list a parent directory via any filename, such as a multiple ..%2F value affecting the 'dodoc' parameter in the /MailAdmin_dll.htm file.
CVE-2023-6277	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB.
CVE-2023-5885	The discontinued FFS Colibri product allows a remote user to access files on the system including files containing login credentials for other users.
CVE-2023-47014	A Cross-Site Request Forgery (CSRF) vulnerability in Sourcecodester Sticky Notes App Using PHP with Source Code v.1.0 allows a local attacker to obtain sensitive information via a crafted payload to add-note.php.
CVE-2023-47755	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AazzTech WooCommerce Product Carousel Slider plugin <= 3.3.5 versions.
CVE-2023-48713	Knative Serving builds on Kubernetes to support deploying and serving of applications and functions as serverless containers. An attacker who controls a pod to a degree where they can control the responses from the /metrics endpoint can cause Denial-of-Service of the autoscaler from an unbound memory allocation bug. This is a DoS vulnerability, where a non-privileged Knative user can cause a DoS for the cluster. This issue has been patched in version 0.39.0.
CVE-2023-5382	The Funnelforms Free plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4. This is due to missing or incorrect nonce validation on the fnsf_delete_posts function. This makes it possible for unauthenticated attackers to delete arbitrary posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

CVE Number	Description
CVE-2023-47786	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LayerSlider plugin <= 7.7.9 versions.
CVE-2023-47808	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Christina Uechi Add Widgets to Page plugin <= 1.3.2 versions.
CVE-2023-5662	The Sponsors plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sponsors' shortcode in all versions up to, and including, 3.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5163	The Weather Atlas Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'shortcode-weather-atlas' shortcode in versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5234	The Related Products for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'woo-related' shortcode in versions up to, and including, 3.3.15 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5664	The Garden Gnome Package plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ggpkg' shortcode in all versions up to, and including, 2.2.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 2.2.7 and fully patched in version 2.2.9.
CVE-2023-5667	The Tab Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5742	The EasyRotator for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'easyrotator' shortcode in all versions up to, and including, 1.0.14 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5338	The Theme Blvd Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.6.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5708	The WP Post Columns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'column' shortcode in all versions up to, and including, 2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-6225	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's su_meta shortcode combined with post meta data in all versions up to, and including, 5.13.3 due to insufficient input sanitization and output escaping on user supplied meta values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5469	The Drop Shadow Boxes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'dropshadowbox' shortcode in versions up to, and including, 1.7.13 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5704	The CPO Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5096	The HTML filter and csv-file search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'csvsearch' shortcode in versions up to, and including, 2.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5128	The TCD Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'map' shortcode in versions up to, and including, 1.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5706	The VK Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vk-blocks/ancestor-page-list' block in all versions up to, and including, 1.63.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-5048	The WDContactFormBuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Contact_Form_Builder' shortcode in versions up to, and including, 1.0.72 due to insufficient input sanitization and output escaping on 'id' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2023-6274	A vulnerability was found in Byzoro Smart S80 up to 20231108. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /sysmanage/updatelib.php of the component PHP File Handler. The manipulation of the argument file_upload leads to unrestricted upload. 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-246103. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-40610	Improper authorization check and possible privilege escalation on Apache Superset up to but excluding 2.1.2. Using the default examples database connection that allows access to both the examples schema and Apache Superset's metadata database, an attacker using a specially crafted CTE SQL statement could change data on the metadata database. This weakness could result on tampering with the authentication/authorization data.

CVE Number	Description
CVE-2023-6008	The UserPro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.1.1. This is due to missing or incorrect nonce validation on multiple functions. This makes it possible for unauthenticated attackers to add, modify, or delete user meta and plugin options.
CVE-2023-6308	A vulnerability, which was classified as critical, has been found in Xiamen Four-Faith Video Surveillance Management System 2016/2017. Affected by this issue is som unknown functionality of the component Apache Struts. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-246134 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but di not respond in any way.
CVE-2023-6307	A vulnerability classified as critical was found in jeecgboot JimuReport up to 1.6.1. Affected by this vulnerability is an unknown functionality of the file /download/image. The manipulation of the argument imageUrl leads to relative path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-246133 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-6306	A vulnerability classified as critical has been found in SourceCodester Free and Open Source Inventory Management System 1.0. Affected is an unknown function of th file /ample/app/ajax/member_data.php. The manipulation of the argument columns 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-246132.
CVE-2023-6305	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file ample/app/ajax/suppliar_data.php. The manipulation of the argument columns leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246131.
CVE-2023-4931	Uncontrolled search path element vulnerability in Plesk Installer affects version 3.27.0.0. A local attacker could execute arbitrary code by injecting DLL files into the same folder where the application is installed, resulting in DLL hijacking in edputil.dll, samlib.dll, urlmon.dll, sspicli.dll, propsys.dll and profapi.dll files.
CVE-2023-6276	A vulnerability classified as critical has been found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file general/wiki/cp/ct/delete.php. The manipulation of the argument PROJ_ID_STR leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-246105 was assigned to this vulnerability.
CVE-2023-25682	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.1 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 247034.
CVE-2023-49029	Cross Site Scripting vulnerability in smpn1smg absis v.2017-10-19 and before allows a remote attacker to execute arbitrary code via the nama parameter in the lock/lock.php file.
CVE-2023-5641	The Martins Free & Easy SEO BackLink Link Building Network WordPress plugin before 1.2.30 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin
CVE-2023-48042	Cross Site Scripting (XSS) in Search filters in Prestashop Amazzing filter version up to version 3.2.5, allows remote attackers to inject arbitrary JavaScript code.
CVE-2023-49215	Usedesk before 1.7.57 allows filter reflected XSS.
CVE-2023-49146	DOMSanitizer (aka dom-sanitizer) before 1.0.7 allows XSS via an SVG document because of mishandling of comments and greedy regular expressions.
CVE-2023-5653	The WassUp Real Time Analytics WordPress plugin through 1.9.4.5 does not escape IP address provided via some headers before outputting them back in an admin page, allowing unauthenticated users to perform Stored XSS attacks against logged in admins
CVE-2023-5958	The POST SMTP Mailer WordPress plugin before 2.7.1 does not escape email message content before displaying it in the backend, allowing an unauthenticated attacker to perform XSS attacks against highly privileged users.
CVE-2023-48034	An issue discovered in Acer Wireless Keyboard SK-9662 allows attacker in physical proximity to both decrypt wireless keystrokes and inject arbitrary keystrokes via use of weak encryption.
CVE-2023-2438	The UserPro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.1.0. This is due to missing or incorrect nonce validation on the 'userpro_save_userdata' function. This makes it possible for unauthenticated attackers to update the user meta and inject malicious JavaScript via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2023-47380	Admidio v4.2.12 and below is vulnerable to Cross Site Scripting (XSS).

CVE Number	Description
CVE-2023-5560	The WP-UserOnline WordPress plugin before 2.88.3 does not sanitise and escape the X-Forwarded-For header before outputting its content on the page, which allows unauthenticated users to perform Cross-Site Scripting attacks.
CVE-2023-5325	The Woocommerce Vietnam Checkout WordPress plugin before 2.0.6 does not escape the custom shipping phone field no the checkout form leading to XSS
CVE-2023-2447	The UserPro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.1.1. This is due to missing or incorrect nonce validation on the 'export_users' function. This makes it possible for unauthenticated attackers to export the users to a csv file, granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2023-4406	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KC Group E-Commerce Software allows Reflected XSS.This issue affects E-Commerce Software: through 20231123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-4594	Stored XSS vulnerability. This vulnerability could allow an attacker to store a malicious JavaScript payload via GET and POST methods on multiple parameters in the MailAdmin_dll.htm file.
CVE-2023-6253	A saved encryption key in the Uninstaller in Digital Guardian's Agent before version 7.9.4 allows a local attacker to retrieve the uninstall key and remove the software by extracting the uninstaller key from the memory of the uninstaller file.
CVE-2023-41787	Uncontrolled Search Path Element vulnerability in Pandora FMS on all allows Leveraging/Manipulating Configuration File Search Paths. This vulnerability allows access to files with sensitive information. This issue affects Pandora FMS: from 700 through 772.
CVE-2023-47829	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codez Quick Call Button plugin <= 1.2.9 versions.
CVE-2023-47759	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Premio Chaty plugin <= 3.1.2 versions.
CVE-2023-49092	RustCrypto/RSA is a portable RSA implementation in pure Rust. Due to a non-constant-time implementation, information about the private key is leaked through timing information which is observable over the network. An attacker may be able to use that information to recover the key. There is currently no fix available. As a workaround, avoid using the RSA crate in settings where attackers are able to observe timing information, e.g. local use on a non-compromised computer.
CVE-2023-47809	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Accordion plugin <= 2.6 versions.
CVE-2021-37937	An issue was found with how API keys are created with the Fleet-Server service account. When an API key is created with a service account, it is possible that the API key could be created with higher privileges than intended. Using this vulnerability, a compromised Fleet-Server service account could escalate themselves to a super-user.
CVE-2023-5981	A vulnerability was found that the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding.
CVE-2023-4642	The kk Star Ratings WordPress plugin before 5.4.6 does not implement atomic operations, allowing one user vote multiple times on a poll due to a Race Condition.
CVE-2023-41792	Cross-Site Request Forgery (CSRF) vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed Javascript code to be executed in the SNMP Trap Editor. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-45286	A race condition in go-resty can result in HTTP request body disclosure across requests. This condition can be triggered by calling sync.Pool.Put with the same *bytes.Buffer more than once, when request retries are enabled and a retry occurs. The call to sync.Pool.Get will then return a bytes.Buffer that hasn't had bytes.Buffer.Reset called on it. This dirty buffer will contain the HTTP request body from an unrelated request, and go-resty will append the current HTTP request body to it, sending two bodies in one request. The sync.Pool in question is defined at package level scope, so a completely unrelated server could receive the request body.
CVE-2023-47833	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress plugin <= 0.18.3 versions.
CVE-2023-42504	An authenticated malicious user could initiate multiple concurrent requests, each requesting multiple dashboard exports, leading to a possible denial of service. This issue affects Apache Superset: before 3.0.0
CVE-2023-32065	OroCommerce is an open-source Business to Business Commerce application built with flexibility in mind. Detailed Order totals information may be received by Order ID. This issue is patched in version 5.0.11 and 5.1.1.

CVE Number	Description
CVE-2023-41812	Unrestricted Upload of File with Dangerous Type vulnerability in Pandora FMS on all allows Accessing Functionality Not Properly Constrained by ACLs. This vulnerability allowed PHP executable files to be uploaded through the file manager. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-6117	A possibility of unwanted server memory consumption was detected through the obsolete functionalities in the Rest API methods of the M-Files server before 23.11.13156.0 which allows attackers to execute DoS attacks.
CVE-2023-3104	Lack of authentication vulnerability. An unauthenticated local user is able to see through the cameras using the web server due to the lack of any form of authentication
CVE-2023-5650	An improper privilege management vulnerability in the ZySH of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an authenticated local attacker to modify the URL of the registration page in the web GUI of an affected device.
CVE-2023-42363	A use-after-free vulnerability was discovered in xasprintf function in xfuncs_printf.c:344 in BusyBox v.1.36.1.
CVE-2023-5960	An improper privilege management vulnerability in the hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.37 and VPN series firmware versions 4.30 through 5.37 could allow an authenticated local attacker to access the system files on an affected device.
CVE-2023-25632	The Android Mobile Whale browser app before 3.0.1.2 allows the attacker to bypass its browser unlock function via 'Open in Whale' feature.
CVE-2023-42364	A use-after-free vulnerability in BusyBox v.1.36.1 allows attackers to cause a denial of service via a crafted awk pattern in the awk.c evaluate function.
CVE-2023-5797	An improper privilege management vulnerability in the debug CLI command of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, VPN series firmware versions 4.30 through 5.37, NWA50AX firmware version 6.29(ABYW.2), WAC500 firmware version 6.65(ABVS.1), WAX300H firmware version 6.60(ACHF.1), and WBE660S firmware version 6.65(ACGG.1), could allow an authenticated local attacker to access the administrator’s logs on an affected device.
CVE-2023-6309	A vulnerability, which was classified as critical, was found in moses-smt mosesdecoder up to 4.0. This affects an unknown part of the file contrib/iSenWeb/trans_result.php. The manipulation of the argument input1 leads to os command injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246135.
CVE-2023-37926	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an authenticated local attacker to cause denial-of-service (DoS) conditions by executing the CLI command to dump system logs on an affected device.
CVE-2023-42365	A use-after-free vulnerability was discovered in BusyBox v.1.36.1 via a crafted awk pattern in the awk.c copyvar function.
CVE-2023-42366	A heap-buffer-overflow was discovered in BusyBox v.1.36.1 in the next_token function at awk.c:1159.
CVE-2023-37925	An improper privilege management vulnerability in the debug CLI command of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, VPN series firmware versions 4.30 through 5.37, NWA50AX firmware version 6.29(ABYW.2), WAC500 firmware version 6.65(ABVS.1), WAX300H firmware version 6.60(ACHF.1), and WBE660S firmware version 6.65(ACGG.1), could allow an authenticated local attacker to access system files on an affected device.
CVE-2023-35136	An improper input validation vulnerability in the “Quagga” package of the Zyxel ATP series firmware versions 4.32 through 5.37, USG FLEX series firmware versions 4.50 through 5.37, USG FLEX 50(W) series firmware versions 4.16 through 5.37, USG20(W)-VPN series firmware versions 4.16 through 5.37, and VPN series firmware versions 4.30 through 5.37, could allow an authenticated local attacker to access configuration files on an affected device.
CVE-2023-43123	On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method File.createTempFile on unix-like systems creates a file with predefined name (so easily identifiable) and by default will create this file with the permissions -rw-r--r--. Thus, if sensitive information is written to this file, other local users can read this information. File.createTempFile(String, String) will create a temporary file in the system temporary directory if the 'java.io.tmpdir' system property is not explicitly set. This affects the class https://github.com/apache/storm/blob/master/storm-core/src/jvm/org/apache/storm/utils/TopologySpoutLag.java#L99 and was introduced by https://issues.apache.org/jira/browse/STORM-3123 In practice, this has a very limited impact as this class is used only if ui.disable.spout.lag.monitoring is set to false, but its value is true by default. Moreover, the temporary file gets deleted soon after its creation. The solution is to use Files.createTempFile https://docs.oracle.com/en/java/javase/11/docs/api/java.base/java/nio/file/Files.html#createTempFile(java.lang.String,java.lang.String,java.nio.file.attribute.FileAttribute... instead. We recommend that all users upgrade to the latest version of Apache Storm.

CVE Number	Description
CVE-2023-20240	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all user of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.
CVE-2023-33202	Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through th PEMParser causes an OutOfMemoryError, which can enable a denial of service attack. (For users of the FIPS Java API: BC-FJA 1.0.2.3 and earlier are affected; BC-FJA 1.0.2.4 is fixed.)
CVE-2023-20241	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all user of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.
CVE-2023-47314	Headwind MDM Web panel 5.22.1 is vulnerable to cross-site scripting (XSS). The file upload function allows APK and arbitrary files to be uploaded. By exploiting this issue, attackers may upload HTML files and share the download URL pointing to these files with the victims. As the file download function returns the file in inline mode the victim's browser will immediately render the content of the HTML file as a web page. As a result, the uploaded client-side code will be evaluated and executed in the victim's browser, allowing attackers to perform common XSS attacks.
CVE-2023-6011	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DECE Software Geodi allows Stored XSS.This issue affects Geodi before 8.0.0.27396.
CVE-2023-26535	Cross-Site Request Forgery (CSRF) vulnerability in WPPOOL Sheets To WP Table Live Sync plugin <= 2.12.15 versions.
CVE-2023-5738	The WordPress Backup & Migration WordPress plugin before 1.4.4 does not sanitise and escape some parameters, which could allow users with a role as low as Subscriber to perform Cross-Site Scripting attacks.
CVE-2023-49216	Usedesk before 1.7.57 allows profile stored XSS.
CVE-2023-28747	Cross-Site Request Forgery (CSRF) vulnerability in codeboxr CBX Currency Converter plugin <= 3.0.3 versions.
CVE-2023-6239	Under rare conditions, the effective permissions of an object might be incorrectly calculated if the object has a specific configuration of metadata-driven permissions in M-Files Server versions 23.9, 23.10, and 23.11 before 23.11.13168.7, potentially enabling unauthorized access to the object.
CVE-2023-49078	raptor-web is a CMS for game server communities that can be used to host information and keep track of players. In version 0.4.4 of raptor-web, it is possible to craft a malicious URL that will result in a reflected cross-site scripting vulnerability. A user controlled URL parameter is loaded into an internal template that has autoescape disabled. This is a cross-site scripting vulnerability that affects all deployments of `raptor-web` on version `0.4.4`. Any victim who clicks on a malicious crafted link will be affected. This issue has been patched 0.4.4.1.
CVE-2023-47313	Headwind MDM Web panel 5.22.1 is vulnerable to Directory Traversal. The application uses an API call to move the uploaded temporary file to the file directory during the file upload process. This API call receives two input parameters, such as path and localPath. The first one refers to the temporary file with an absolute path without validating it. Attackers may modify this API call by referring to arbitrary files. As a result, arbitrary files can be moved to the files directory and so they can be downloaded.
CVE-2023-47758	Cross-Site Request Forgery (CSRF) vulnerability in Mondula GmbH Multi Step Form plugin <= 1.7.11 versions.
CVE-2023-47316	Headwind MDM Web panel 5.22.1 is vulnerable to Incorrect Access Control. The Web panel allows users to gain access to potentially sensitive API calls such as listing users and their data, file management API calls and audit-related API calls.
CVE-2023-49028	Cross Site Scripting vulnerability in smpn1smg absis v.2017-10-19 and before allows a remote attacker to execute arbitrary code via the user parameter in the lock/lock.php file.
CVE-2023-27442	Cross-Site Request Forgery (CSRF) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.29.2 versions.
CVE-2023-5620	The Web Push Notifications WordPress plugin before 4.35.0 does not prevent visitors on the site from changing some of the plugin options, some of which may be used to conduct Stored XSS attacks.

CVE Number	Description
CVE-2023-4514	The Mmm Simple File List WordPress plugin through 2.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks
CVE-2023-5942	The Medialist WordPress plugin before 1.4.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks
CVE-2023-6359	A Cross-Site Scripting (XSS) vulnerability has been found in Alumne LMS affecting version 4.0.0.1.08. An attacker could exploit the 'localidad' parameter to inject a custom JavaScript payload and partially take over another user's browser session, due to the lack of proper sanitisation of the 'localidad' field on the /users/editmy page
CVE-2023-26532	Cross-Site Request Forgery (CSRF) vulnerability in AccessPress Themes Social Auto Poster plugin <= 2.1.4 versions.
CVE-2023-39925	Cross-Site Request Forgery (CSRF) vulnerability in PeepSo Download Community by PeepSo plugin <= 6.1.6.0 versions.
CVE-2023-47437	A vulnerability has been identified in Pachno 1.0.6 allowing an authenticated attacker to execute a cross-site scripting (XSS) attack. The vulnerability exists due to inadequate input validation in the Project Description and comments, which enables an attacker to inject malicious java script.
CVE-2023-29060	The FACSChorus workstation operating system does not restrict what devices can interact with its USB ports. If exploited, a threat actor with physical access to the workstation could gain access to system information and potentially exfiltrate data.
CVE-2023-27453	Cross-Site Request Forgery (CSRF) vulnerability in LWS LWS Tools plugin <= 2.3.1 versions.
CVE-2023-26542	Cross-Site Request Forgery (CSRF) vulnerability in Exeebit phpinfo() WP plugin <= 4.0 versions.
CVE-2023-47824	Cross-Site Request Forgery (CSRF) vulnerability in wpWax Legal Pages – Privacy Policy, Terms & Conditions, GDPR, CCPA, and Cookie Notice Generator plugin <= 1.3.8 versions.
CVE-2023-5611	The Seraphinite Accelerator WordPress plugin before 2.20.32 does not have authorisation and CSRF checks when resetting and importing its settings, allowing unauthenticated users to reset them
CVE-2023-49321	Certain WithSecure products allow a Denial of Service because scanning a crafted file takes a long time, and causes the scanner to hang. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Clier Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, WithSecure Linux Security 64 12.0, WithSecure Linux Protection 12.0, and WithSecure Atlant 1.0.35-1.
CVE-2023-4252	The EventPrime WordPress plugin through 3.2.9 specifies the price of a booking in the client request, allowing an attacker to purchase bookings without payment.
CVE-2023-47392	An access control issue in Mercedes me IOS APP v1.34.0 and below allows attackers to view the carts of other users via sending a crafted add order request.
CVE-2023-46355	In the module "CSV Feeds PRO" (csvfeeds) < 2.6.1 from Bl Modules for PrestaShop, a guest can download personal information without restriction. Due to too permissive access control which does not force administrator to use password on feeds, a guest can access exports from the module which can lead to leaks of personal information from ps_customer / ps_order table such as name / surname / email / phone number / postal address.
CVE-2023-47668	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StellarWP Membership Plugin – Restrict Content plugin <= 3.2.7 versions.
CVE-2023-34053	In Spring Framework versions 6.0.0 - 6.0.13, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC or Spring WebFlux * io.micrometer:micrometer-core is on the classpath * an ObservationRegistry is configured in the application to record observations Typically, Spring Boot applications need the org.springframework.boot:spring-boot-actuator dependency to meet all conditions.
CVE-2023-34054	In Reactor Netty HTTP Server, versions 1.1.x prior to 1.1.13 and versions 1.0.x prior to 1.0.39, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable if Reactor Netty HTTP Server built-in integration with Micrometer is enabled.
CVE-2023-6264	Information leak in Content-Security-Policy header in Devolutions Server 2023.3.7.0 allows an unauthenticated attacker to list the configured Devolutions Gateways endpoints.

CVE Number	Description
CVE-2023-34055	In Spring Boot versions 2.7.0 - 2.7.17, 3.0.0-3.0.12 and 3.1.0-3.1.5, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-servic (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC or Spring WebFlux * org.springframework.boot:spring-boot-actuator is on the classpath
CVE-2023-48121	An authentication bypass vulnerability in the Direct Connection Module in Ezviz CS-C6N-xxx prior to v5.3.x build 20230401, Ezviz CS-CV310-xxx prior to v5.3.x build 20230401, Ezviz CS-C6CN-xxx prior to v5.3.x build 20230401, Ezviz CS-C3N-xxx prior to v5.3.x build 20230401 allows remote attackers to obtain sensitive information by sending crafted messages to the affected devices.
CVE-2023-41145	Autodesk users who no longer have an active license for an account can still access cases for that account.
CVE-2023-30588	When an invalid public key is used to create an x509 certificate using the crypto.X509Certificate() API a non-expect termination occurs making it susceptible to DoS attacks when the attacker could force interruptions of application processing, as the process terminates when accessing public key info of provided certificates from use code. The current context of the users will be gone, and that will cause a DoS scenario. This vulnerability affects all active Node.js versions v16, v18, and, v20.
CVE-2023-47244	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Omnisend Email Marketing for WooCommerce by Omnisend.This issue affects Email Marketing for WooCommerce by Omnisend: from n/a through 1.13.8.
CVE-2023-5871	A flaw was found in libnbd, due to a malicious Network Block Device (NBD), a protocol for accessing Block Devices such as hard disks over a Network. This issue may allow a malicious NBD server to cause a Denial of Service.
CVE-2023-47529	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ThemeIsle Cloud Templates & Patterns collection.This issue affects Cloud Templates & Patterns collection: from n/a through 1.2.2.
CVE-2023-5845	The Simple Social Media Share Buttons WordPress plugin before 5.1.1 leaks password-protected post content to unauthenticated visitors in some meta tags
CVE-2023-47393	An access control issue in Mercedes me IOS APP v1.34.0 and below allows attackers to view the maintenance orders of other users and access sensitive user information via unspecified vectors.
CVE-2023-41811	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed Javascript code to be executed in the news section of the web console. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-35139	A cross-site scripting (XSS) vulnerability in the CGI program of the Zyxel ATP series firmware versions 5.10 through 5.37, USG FLEX series firmware versions 5.00 through 5.37, USG FLEX 50(W) series firmware versions 5.10 through 5.37, USG20(W)-VPN series firmware versions 5.10 through 5.37, and VPN series firmware versions 5.00 through 5.37, could allow an unauthenticated LAN-based attacker to store malicious scripts in a vulnerable device. A successful XSS attack could then result in the stored malicious scripts being executed to steal cookies when the user visits the specific CGI used for dumping ZTP logs.
CVE-2023-29061	There is no BIOS password on the FACSChorus workstation. A threat actor with physical access to the workstation can potentially exploit this vulnerability to access th BIOS configuration and modify the drive boot order and BIOS pre-boot authentication.
CVE-2023-32062	OroPlatform is a package that assists system and user calendar management. Back-office users can access information from any system calendar event, bypassing ACL security restrictions due to insufficient security checks. This vulnerability has been patched in version 5.1.1.
CVE-2023-48707	CodeIgniter Shield is an authentication and authorization provider for CodeIgniter 4. The `secretKey` value is an important key for HMAC SHA256 authentication and in affected versions was stored in the database in cleartext form. If a malicious person somehow had access to the data in the database, they could use the key and secretKey for HMAC SHA256 authentication to send requests impersonating that corresponding user. This issue has been addressed in version 1.0.0-beta.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2023-32064	OroCommerce package with customer portal and non authenticated visitor website base features. Back-office users can access information about Customer and Customer User menus, bypassing ACL security restrictions due to insufficient security checks. This issue has been patched in version 5.0.11 and 5.1.1.
CVE-2023-48708	CodeIgniter Shield is an authentication and authorization provider for CodeIgniter 4. In affected versions successful login attempts are recorded with the raw tokens stored in the log table. If a malicious person somehow views the data in the log table they can obtain a raw token which can then be used to send a request with that user's authority. This issue has been addressed in version 1.0.0-beta.8. Users are advised to upgrade. Users unable to upgrade should disable logging for successful login attempts by the configuration files.
CVE-2023-20084	A vulnerability in the endpoint software of Cisco Secure Endpoint for Windows could allow an authenticated, local attacker to evade endpoint protection within a limited time window. This vulnerability is due to a timing issue that occurs between various software components. An attacker could exploit this vulnerability by persuading a user to put a malicious file into a specific folder and then persuading the user to execute the file within a limited time window. A successful exploit could allow the attacker to cause the endpoint software to fail to quarantine the malicious file or kill its process. Note: This vulnerability only applies to deployments that have the Windows Folder Redirection feature enabled.
CVE-2023-32063	OroCalendarBundle enables a Calendar feature and related functionality in Oro applications. Back-office users can access information from any call event, bypassing ACL security restrictions due to insufficient security checks. This issue has been patched in version 5.0.4 and 5.1.1.

CVE Number	Description
CVE-2023-5209	The WordPress Online Booking and Scheduling Plugin WordPress plugin before 22.5 does not sanitise and escape some of its settings, which could allow high privileg users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)
CVE-2023-42502	An authenticated attacker with update datasets permission could change a dataset link to an untrusted site by spoofing the HTTP Host header, users could be redirecte to this site when clicking on that specific dataset. This issue affects Apache Superset versions before 3.0.0.
CVE-2023-2707	The gAppointments WordPress plugin through 1.9.5.1 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)
CVE-2023-6312	A vulnerability was found in SourceCodester Loan Management System 1.0. It has been classified as critical. Affected is the function delete_user of the file deleteUser.php of the component Users Page. The manipulation of the argument user_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-246138 is the identifier assigned to this vulnerability.
CVE-2023-6311	A vulnerability was found in SourceCodester Loan Management System 1.0 and classified as critical. This issue affects the function delete_ltype of the file delete_ltype.php of the component Loan Type Page. The manipulation of the argument ltype_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-246137 was assigned to this vulnerability.
CVE-2023-6302	A vulnerability was found in CSZCMS 1.3.0 and classified as critical. Affected by this issue is some unknown functionality of the file \views\templates of the component File Manager Page. The manipulation leads to permission issues. 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-246128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-6310	A vulnerability has been found in SourceCodester Loan Management System 1.0 and classified as critical. This vulnerability affects the function delete_borrower of the file deleteBorrower.php. The manipulation of the argument borrower_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-246136.
CVE-2023-4397	A buffer overflow vulnerability in the Zyxel ATP series firmware version 5.37, USG FLEX series firmware version 5.37, USG FLEX 50(W) series firmware version 5.37, and USG20(W)-VPN series firmware version 5.37, could allow an authenticated local attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing the CLI command with crafted strings on an affected device.
CVE-2023-5715	The Website Optimization – Plerdy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's tracking code settings in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.
CVE-2023-4726	The Ultimate Dashboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 3.7.7. due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disable
CVE-2023-5383	The Funnelforms Free plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4. This is due to missing or incorrect nonce validation on the fnsf_copy_posts function. This makes it possible for unauthenticated attackers to create copies of arbitrary posts via a forged request granted they car trick a site administrator into performing an action such as clicking on a link.
CVE-2022-35638	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.1 is vulnerable to cross-site request forgery which could allow an attacke to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 230824.
CVE-2023-4686	The WP Customer Reviews plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 3.6.6 via the ajax_enabled_posts function. This can allow authenticated attackers to extract sensitive data such as post titles and slugs, including those of protected and trashed posts and pages in addition to other post types such as galleries.
CVE-2023-5387	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_af2_trigger_dark_mode function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to enable or disable the dark mode plugin setting.
CVE-2023-41146	Autodesk Customer Support Portal allows cases created by users under an account to see cases created by other users on the same account.
CVE-2023-5411	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_af2_save_post function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify certain post values. Note that the extent of modification is limited due to fixed values passed to the wp_update_post function.
CVE-2023-5415	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_add_category function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to add new categories.
CVE-2023-6226	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.13.3 vi the su_meta shortcode due to missing validation on the user controlled keys 'key' and 'post_id'. This makes it possible for authenticated attackers, with contributor-level access and above, to retrieve arbitrary post meta values which may contain sensitive information when combined with another plugin.
CVE-2023-42505	An authenticated user with read permissions on database connections metadata could potentially access sensitive information such as the connection's username. This issue affects Apache Superset before 3.0.0.

CVE Number	Description
CVE-2023-5419	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_af2_test_mail function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to send test emails to an arbitrary email address.
CVE-2023-5314	The WP EXtra plugin for WordPress is vulnerable to unauthorized access to restricted functionality due to a missing capability check on the 'test-email' section of the register() function in versions up to, and including, 6.2. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to send email with arbitrary content to arbitrary locations from the affected site's mail server.
CVE-2023-5416	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_delete_category function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete categories.
CVE-2023-5417	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_update_category function i versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify the Funnelforms category for a given post ID.
CVE-2023-5385	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_copy_posts function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to create copies of arbitrary posts.
CVE-2023-47775	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team Comments — wpDiscuz plugin <= 7.6.11 versions.
CVE-2023-48268	Mattermost fails to limit the amount of data extracted from compressed archives during board import in Mattermost Boards allowing an attacker to consume excessive resources, possibly leading to Denial of Service, by importing a board using a specially crafted zip (zip bomb).
CVE-2023-6297	A vulnerability classified as problematic has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file patient-search-report.php of the component Search Report Page. The manipulation of the argument Search By Patient Name with the input <script>alert(document.cookie) </script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifi of this vulnerability is VDB-246123.
CVE-2022-36777	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.16.0could allow an authenticated user to obtain sensitive version information that could aid in further attacks against the system. IBM X-Force ID: 233665.
CVE-2023-27457	Cross-Site Request Forgery (CSRF) vulnerability in Passionate Brains Add Expires Headers & Optimized Minify plugin <= 2.7 versions.
CVE-2023-27446	Cross-Site Request Forgery (CSRF) vulnerability in Fluenx DeepL API translation plugin <= 2.1.4 versions.
CVE-2023-47765	Cross-Site Request Forgery (CSRF) vulnerability in CodeBard CodeBard's Patron Button and Widgets for Patreon plugin <= 2.1.9 versions.
CVE-2023-6299	A vulnerability, which was classified as problematic, has been found in Apryse iText 8.0.1. This issue affects some unknown processing of the file PdfDocument.java of the component Reference Table Handler. The manipulation leads to memory leak. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 8.0.2 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-246125 was assigned to this vulnerability. NOTE: The vendor was contacted early about this vulnerability. The fix was introduced in the iText 8.0.2 release on October 25th 2023, prior to the disclosure.
CVE-2023-6298	A vulnerability classified as problematic was found in Apryse iText 8.0.2. This vulnerability affects the function main of the file PdfDocument.java. The manipulation lead to improper validation of array index. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier of this vulnerability is VDB-246124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. A statement published afterwards explains that the exception is not a vulnerability and the identified CWEs might not apply to the software.
CVE-2023-6296	A vulnerability was found in osCommerce 4. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /catalog/compare of the component Instant Message Handler. The manipulation of the argument compare with the input 40dz4iq"><script>alert(1)</script>zohkx leads to cross site scripting. The attack may be launched remotely. VDB-246122 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-47825	Cross-Site Request Forgery (CSRF) vulnerability in TienCOP WP EXtra plugin <= 6.4 versions.
CVE-2023-27444	Cross-Site Request Forgery (CSRF) vulnerability in Pierre Lannoy / PerfOps One DecaLog plugin <= 3.7.0 versions.
CVE-2023-23978	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in SwitchWP WP Client Reports plugin <= 1.0.16 versions.

CVE Number	Description
CVE-2023-27458	Cross-Site Request Forgery (CSRF) vulnerability in wpstream WpStream plugin <= 4.4.10 versions.
CVE-2023-27461	Cross-Site Request Forgery (CSRF) vulnerability in Yoohoo Plugins When Last Login plugin <= 1.2.1 versions.
CVE-2023-25987	Cross-Site Request Forgery (CSRF) vulnerability in Aleksandar Urošević My YouTube Channel plugin <= 3.23.3 versions.
CVE-2023-25986	Cross-Site Request Forgery (CSRF) vulnerability in WattIsIt PayGreen – Ancienne version plugin <= 4.10.2 versions.
CVE-2023-47865	Mattermost fails to check if hardened mode is enabled when overriding the username and/or the icon when posting a post. If settings allowed integrations to override th username and profile picture when posting, a member could also override the username and icon when making a post even if the Hardened Mode setting was enabled
CVE-2023-40703	Mattermost fails to properly limit the characters allowed in different fields of a block in Mattermost Boards allowing a attacker to consume excessive resources, possibly leading to Denial of Service, by patching the field of a block using a specially crafted string.
CVE-2023-28749	Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM On Demand Search And Replace plugin <= 1.3.0 versions.
CVE-2023-47819	Cross-Site Request Forgery (CSRF) vulnerability in Dang Ngoc Binh Easy Call Now by ThikShare plugin <= 1.1.0 versions.
CVE-2023-47792	Cross-Site Request Forgery (CSRF) vulnerability in Infinite Uploads Big File Uploads – Increase Maximum File Upload Size plugin <= 2.1.1 versions.
CVE-2023-5537	The Delete Usermeta plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing nonce validation on the delumet_options_page() function. This makes it possible for unauthenticated attackers to remove user meta for arbitrary users via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2023-5737	The WordPress Backup & Migration WordPress plugin before 1.4.4 does not authorize some AJAX requests, allowing users with a role as low as Subscriber to update some plugin settings.
CVE-2023-5525	The Limit Login Attempts Reloaded WordPress plugin before 2.25.26 is missing authorization on the `toggle_auto_update` AJAX action, allowing any user with a valid nonce to toggle the auto-update status of the plugin.
CVE-2023-4297	The Mmm Simple File List WordPress plugin through 2.3 does not validate the generated path to list files from, allowing any authenticated users, such as subscribers, t list the content of arbitrary directories.
CVE-2023-6189	Missing access permissions checks in the M-Files server before 23.11.13156.0 allow attackers to perform data write and export jobs using the M-Files API methods.
CVE-2023-43701	Improper payload validation and an improper REST API response type, made it possible for an authenticated malicious actor to store malicious code into Chart's metadata, this code could get executed if a user specifically accesses a specific deprecated API endpoint. This issue affects Apache Superset versions prior to 2.1.2. Users are recommended to upgrade to version 2.1.2, which fixes this issue.
CVE-2023-43754	Mattermost fails to check whether the “Allow users to view archived channels” setting is enabled during permalink previews display, allowing members to view permalink previews of archived channels even if the “Allow users to view archived channels” setting is disabled.
CVE-2023-42501	Unnecessary read permissions within the Gamma role would allow authenticated users to read configured CSS templates and annotations. This issue affects Apache Superset: before 2.1.2. Users should upgrade to version or above 2.1.2 and run `superset init` to reconstruct the Gamma role or remove `can_read` permission from th mentioned resources.
CVE-2023-6202	Mattermost fails to perform proper authorization in the /plugins/focalboard/api/v2/users endpoint allowing an attacker who is a guest user and knows the ID of another user to get their information (e.g. name, surname, nickname) via Mattermost Boards.
CVE-2023-48369	Mattermost fails to limit the log size of server logs allowing an attacker sending specially crafted requests to different endpoints to potentially overflow the log.

CVE Number	Description
CVE-2023-47791	Cross-Site Request Forgery (CSRF) vulnerability in Leadster plugin <= 1.1.2 versions.
CVE-2023-47168	Mattermost fails to properly check a redirect URL parameter allowing for an open redirect was possible when the user clicked "Back to Mattermost" after providing a invalid custom url scheme in /oauth/{service}/mobile_login?redirect_to=
CVE-2023-45223	Mattermost fails to properly validate the "Show Full Name" option in a few endpoints in Mattermost Boards, allowing a member to get the full name of another user ever if the Show Full Name option was disabled.
CVE-2023-27633	Cross-Site Request Forgery (CSRF) vulnerability in Pixelgrade Customify – Intuitive Website Styling plugin <= 2.10.4 versions.
CVE-2023-29064	The FACSChorus software contains sensitive information stored in plaintext. A threat actor could gain hardcoded secrets used by the application, which include tokens and passwords for administrative accounts.
CVE-2023-29065	The FACSChorus software database can be accessed directly with the privileges of the currently logged-in user. A threat actor with physical access could potentially gain credentials, which could be used to alter or destroy data stored in the database.
CVE-2023-43081	PowerProtect Agent for File System Version 19.14 and prior, contains an incorrect default permissions vulnerability in ddfscon component. A low Privileged local attacker could potentially exploit this vulnerability, leading to overwriting of log files.
CVE-2023-41810	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed Javascript code to be executed in some Widgets' text box. This issue affects Pandora FMS: from 700 through 773.
CVE-2023-29062	The Operating System hosting the FACSChorus application is configured to allow transmission of hashed user credentials upon user action without adequately validating the identity of the requested resource. This is possible through the use of LLMNR, MBT-NS, or MDNS and will result in NTLMv2 hashes being sent to a malicious entity position on the local network. These hashes can subsequently be attacked through brute force and cracked if a weak password is used. This attack would only apply to domain joined systems.
CVE-2023-48711	google-translate-api-browser is an npm package which interfaces with the google translate web api. A Server-Side Request Forgery (SSRF) Vulnerability is present in applications utilizing the `google-translate-api-browser` package and exposing the `translateOptions` to the end user. An attacker can set a malicious `tld`, causing the application to return unsafe URLs pointing towards local resources. The `translateOptions.tld` field is not properly sanitized before being placed in the Google translate URL. This can allow an attacker with control over the `translateOptions` to set the `tld` to a payload such as `@127.0.0.1`. This causes the full URL to become `https://translate.google.@127.0.0.1/...`, where `translate.google.` is the username used to connect to localhost. An attacker can send requests within internal networks and the local host. Should any HTTPS application be present on the internal network with a vulnerability exploitable via a GET call, then it would be possible to exploit this using this vulnerability. This issue has been addressed in release version 4.1.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2023-48706	Vim is a UNIX editor that, prior to version 9.0.2121, has a heap-use-after-free vulnerability. When executing a `:s` command for the very first time and using a sub-replace-special atom inside the substitution part, it is possible that the recursive `:s` call causes free-ing of memory which may later then be accessed by the initial `:s` command. The user must intentionally execute the payload and the whole process is a bit tricky to do since it seems to work only reliably for the very first :s command. may also cause a crash of Vim. Version 9.0.2121 contains a fix for this issue.
CVE-2023-6300	A vulnerability, which was classified as problematic, was found in SourceCodester Best Courier Management System 1.0. Affected is an unknown function. The manipulation of the argument page with the input </TiTlE><ScRiPt>alert(1)</ScRiPt> leads to cross site scripting. It is possible to launch the attack remotely. The explo has been disclosed to the public and may be used. VDB-246126 is the identifier assigned to this vulnerability.
CVE-2023-6301	A vulnerability has been found in SourceCodester Best Courier Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file parcel_list.php of the component GET Parameter Handler. The manipulation of the argument id with the input </TiTlE><ScRiPt>alert(1)</ScRiPt> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246127.
CVE-2023-6313	A vulnerability was found in SourceCodester URL Shortener 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Long URL Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246139.
CVE-2023-6251	Cross-site Request Forgery (CSRF) in Checkmk < 2.2.0p15, < 2.1.0p37, <= 2.0.0p39 allow an authenticated attacker to delete user-messages for individual users.
CVE-2023-6275	A vulnerability was found in TOTVS Fluig Platform 1.6.x/1.7.x/1.8.0/1.8.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /mobileredir/openApp.jsp of the component mobileredir. The manipulation of the argument redirectUrl/user with the input "><script>alert(document.domain)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.7.1-231128, 1.8.0-231127 and 1.8.1-231127 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-246104.
CVE-2023-6287	Sensitive data exposure in Webconf in Tribe29 Checkmk Appliance before 1.6.8 allows local attacker to retrieve passwords via reading log files.

CVE Number	Description
CVE-2023-6160	The LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 7.4.2 via the maybe_serve_export function. This makes it possible for authenticated attackers, with administrator or LMS manager access and above, to read the contents of arbitrar CSV files on the server, which can contain sensitive information as well as removing those files from the server.
CVE-2023-26279	IBM QRadar WinCollect Agent 10.0 through 10.1.7 could allow a local user to perform unauthorized actions due to improper encoding. IBM X-Force ID: 248160.
CVE-2023-29066	The FACSChorus software does not properly assign data access privileges for operating system user accounts. A non-administrative OS account can modify information stored in the local application data folders.
CVE-2023-35075	Mattermost fails to use innerText / textContent when setting the channel name in the webapp during autocomplete, allowing an attacker to inject HTML to a victim's page by create a channel name that is valid HTML. No XSS is possible though.
CVE-2021-22151	It was discovered that Kibana was not validating a user supplied path, which would load .pbf files. Because of this, a malicious user could arbitrarily traverse the Kibana host to load internal files ending in the .pbf extension.
CVE-2021-39008	IBM QRadar WinCollect Agent 10.0 through 10.1.7 could allow a privileged user to obtain sensitive information due to missing best practices. IBM X-Force ID: 213551.
CVE-2023-6303	A vulnerability was found in CSZCMS 1.3.0. It has been classified as problematic. This affects an unknown part of the file /admin/settings/ of the component Site Settings Page. The manipulation of the argument Additional Meta Tag with the input <svg><animate onbegin=alert(1) attributeName=x dur=1s> 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 identifier VDB-246129 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-29063	The FACSChorus workstation does not prevent physical access to its PCI express (PCIe) slots, which could allow a threat actor to insert a PCI card designed for memory capture. A threat actor can then isolate sensitive information such as a BitLocker encryption key from a dump of the workstation RAM during startup.
CVE-2023-6164	The MainWP Dashboard – WordPress Manager for Multiple Websites Maintenance plugin for WordPress is vulnerable to CSS Injection via the ‘newColor’ parameter in all versions up to, and including, 4.5.1.2 due to insufficient input sanitization. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary CSS values into the site tags.
CVE-2021-22143	The Elastic APM .NET Agent can leak sensitive HTTP header information when logging the details during an application error. Normally, the APM agent will sanitize sensitive HTTP header details before sending the information to the APM server. During an application error it is possible the headers will not be sanitized before being sent.
CVE-2024-0070	Rejected reason: This CVE ID was unused by the CNA.
CVE-2024-0069	Rejected reason: This CVE ID was unused by the CNA.
CVE-2023-5773	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-6136. Reason: This record is a reservation duplicate of CVE-20nn-nnnn. Notes: All CVE users should reference CVE-2023-6136 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.
CVE-2023-38914	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that was not a security issue. Notes: none.